EDITORIAL VISIÓN CONJUNTA . BIBLIOTECA CONJUNTA

OPERACIONES MILITARES CIBERNÉTICAS

Planeamiento y Ejecución en el Nivel Operacional

General de División (RE) **Evergisto de Vergara**
Contraalmirante (RE) **Gustavo Adolfo Trama**

Escuela Superior de Guerra Conjunta de las Fuerzas Armadas

OPERACIONES MILITARES CIBERNÉTICAS

Planeamiento y Ejecución en el Nivel Operacional

Escuela Superior de Guerra Conjunta
Editorial Visión Conjunta

BIBLIOTECA CONJUNTA

DIRECTOR
Brigadier Fabián Otero

EDITOR Y PROPIETARIO
Escuela Superior de Guerra Conjunta de las Fuerzas Armadas

Av. Luis María Campos 480, 2° piso, CI1426BOP, CABA

> visionconjunta-esgc@fuerzas-armadas.mil.ar

Autores
General de División (RE) **Evergisto de Vergara**
Contraalmirante (RE) **Gustavo Adolfo Trama**

Colaboradores
Brigadier (RE) **Marcelo Noel Uriona**
Doctor **Javier Ulises Ortiz**

Asesora Metodológica
Dra. **Lucía Alejandra Destro**

OPERACIONES MILITARES CIBERNÉTICAS

Planeamiento y Ejecución en el Nivel Operacional

Escuela Superior de Guerra Conjunta de las Fuerzas Armadas

Trama, Gustavo Adolfo
Operaciones militares cibernéticas : planeamiento y ejecución en el nivel operacional / Gustavo Adolfo Trama ; Evergisto Arturo de Vergara. - 1a ed . - Ciudad Autónoma de Buenos Aires : Escuela Superior de Guerra Conjunta de las Fuerzas Armadas, 2017.
270 p. ; 23 x 16 cm.

ISBN: 978-987-29264-7-2

1. Estrategia Militar. 2. Conflictos Bélicos. I. Vergara, Evergisto Arturo de II. Título
CDD 355.4

Fecha de catalogación: 11/12/17

ISBN: 978-987-29264-4-1

Queda hecho el depósito que previene la Ley 11.723
Buenos Aires, diciembre de 2017

Este escrito es presentado en cumplimiento parcial de los requerimientos de la Secretaría de Investigación de la Escuela Superior de Guerra Conjunta. Las opiniones expresadas son propias de los autores y no reflejan las políticas o posturas de las Fuerzas Armadas de la República Argentina, del Ministerio de Defensa o del Gobierno Nacional.

ÍNDICE

PRESENTACIÓN

Los aspectos que influyen en la vida diaria con respecto al uso del espacio cibernético tienen amplia difusión. Todas las acciones que se desarrollen en este campo afectarán al componente armado del poder nacional desde varias perspectivas.

La primera de ellas es el uso de la fuerza convencional militar como respuesta a un ataque cibernético masivo. Se contempla esta posibilidad porque los países más poderosos en aplicaciones cibernéticas de uso diario son justamente los más vulnerables en este aspecto. Se dice que los efectos de un ataque masivo cibernético multiplicado varias veces a lo ocurrido en Estonia en el año 2007 tendrían los mismos resultados devastadores que un ataque nuclear. No todos los países adhieren a esta postura porque daría lugar al uso arbitrario de la fuerza convencional por causas que luego originarían disculpas efusivas, pero sin efectos que puedan retrotraerse.

La segunda implica el uso del poder militar convencional de los países ante el ataque cibernético a infraestructuras civiles. Las consecuencias sobre la población civil de un ataque a las infraestructuras críticas[1] podrán requerir el empleo inmediato de fuerzas militares para paliar los efectos en tareas que seguramente excederán a la ayuda humanitaria, como por ejemplo la prevención de saqueos y vandalismos. Este empleo militar forzoso en ayuda humanitaria puede, además, complementarse con un ataque militar convencional al país afectado, ya que distraerá tropas de otros lugares.

La tercera acción tiene dos facetas: la primera de ellas es la lucha entre redes y sistemas de redes para afectar, en operaciones cibernéticas defensivas - activas y pasivas - y de exploración, el uso de los sistemas automatizados de comando y control que proporcionan poder de combate a las fuerzas militares enemigas. La segunda es el uso del espacio cibernético como herramienta para las operaciones de información que buscan engañar al enemigo para que tome decisiones erróneas. En estas operaciones de información, la cibernética puede ser usada en operaciones de apoyo de información a las operaciones mi-

1 Art. 5.° Las Partes convienen en que un ataque armado contra una o varias de ellas, ocurrido en Europa o en América del Norte, será considerado como un ataque dirigido contra todas, y, en consecuencia, convienen en que si tal ataque se produce, cada una de ellas, en el ejercicio del derecho de legítima defensa, individual o colectiva, reconocido por el art. 51 de la Carta de las Naciones Unidas, asistirá a la Parte o Partes atacadas tomando individualmente, y de acuerdo con las otras, las medidas que juzgue necesarias, comprendido el empleo de las fuerzas armadas para restablecer la seguridad en la región del Atlántico Norte.

litares (MISO – ex operaciones psicológicas), de engaño militar, de guerra electrónica y en operaciones de inteligencia tales como el espionaje y descifrado de claves.

En esta obra se profundiza en el uso e influencia de la cibernética en las operaciones militares convencionales y, específicamente, en los aspectos que deben tenerse en cuenta en el nivel operacional de guerra, cuando llega el momento de implementar la dirección estratégica.

El desarrollo del espacio cibernético aún es incipiente y evoluciona día a día. Por las características únicas de este ámbito ya se puede hablar de un nuevo ambiente que ha de sumarse a los conocidos de aire, espacio, mar y tierra. La Organización del Tratado del Atlántico Norte ha declarado oficialmente el 16 de junio de 2016 al espacio cibernético como una zona de guerra; lo cual significa que los ataques llevados a cabo en este contexto podrían desencadenar una respuesta del artículo 5 del Tratado del Atlántico Norte[1]. Por su parte, Estados Unidos ya ha aceptado que el espacio cibernético es la quinta dimensión en el uso de fuerzas militares.

La perspectiva que se sostiene en esta investigación es que, en el nivel operacional el espacio cibernético debe ser incluido junto a los ambientes tradicionales de aire, espacio, mar y tierra. Por esta razón, un Comandante de un Teatro de Operaciones debe saber cómo incorporarlo al método de planeamiento y qué requerir de él en la ejecución de operaciones militares bajo su responsabilidad.

Palabras clave: Espacio cibernético – Ciberseguridad y Ciberdefensa – Teatro de Operaciones -Planeamiento y Ejecución – Operaciones Cibernéticas Militares – Operaciones de Información.

INTRODUCCIÓN

Los adelantos tecnológicos y la creciente infraestructura digital han hecho que poblaciones enteras dependan de sistemas entrelazados y complejos. La demanda de Internet y de conectividad digital exige una integración cada vez mayor de las Tecnologías de la Información y la Comunicación (TIC) en productos que anteriormente funcionaban sin estas técnicas, como por ejemplo sistemas de control de represas, sistemas de control de tránsito, sistemas de salud nacionales integrados, redes de distribución eléctrica, redes sanitarias de agua corriente y cloacas y de transporte polimodal, movimientos y tráfico aéreo, reservas de pasajes, movimientos bancarios como trasferencias y pagos bancarios, pagos en comercios, depósito de sueldos, y hasta de estacionamiento pago. En los países desarrollados, prácticamente todos los servicios modernos dependen de la utilización de las TIC.

A medida que fue aumentando la dependencia respecto de ellas, en el plano mundial también se incrementó la vulnerabilidad a los ataques contra las infraestructuras críticas[2] a través del espacio cibernético, entendiendo por este (aunque, como se verá más adelante, hay una multiplicidad de definiciones del concepto) al dominio virtual, global y dinámico, creado por el hombre, compuesto por las infraestructuras de tecnología de la información, las redes y los sistemas de información y de telecomunicaciones, incluidas las de las Fuerzas Armadas.

El espacio cibernético, junto con los tradicionales ambientes terrestre, marítimo, aéreo y espacial es objeto de análisis por parte de numerosas instituciones públicas y privadas, tanto nacionales como internacionales. Esto puede demostrarse si se observa a las instituciones universales y regionales de seguridad como la ONU[3], la OEA[4], la NATO[5] y la

2 Aquellas instalaciones, redes, servicios y equipos físicos y de tecnología de la información cuya interrupción o destrucción tendría un impacto mayor en la salud, la seguridad o el bienestar económico de los ciudadanos o en el eficaz funcionamiento de las instituciones del Estado y de las Administraciones Públicas". Esta definición fue establecida por la Directiva europea: 2008/114/CE del 8 de diciembre de 2008.

3 United Nations, Cybersecurity a global issue demanding a global approach; Disponible en: http://www.un.org/en/development/desa/news/ecosoc/cybersecurity-demands-global-approach.html

4 Organization of American States, Cybersecurity Programme; Disponible en: http://www.oas.org/en/topics/cyber_security.asp

5 North Atlantic Treaty, Organization Cyber Defence; Disponible en: http://www.nato.int/cps/en/natohq/topics_78170.htm

OSCE[6] que han incorporado en sus estructuras a organismos competentes sobre el tema, así como diversos países que han incluido la problemática del espacio cibernético a sus agendas de estrategia nacional de seguridad[7] ya que los incidentes y los ataques cibernéticos se han convertido en una fuente de amenazas en el mundo globalizado, debido a su capacidad de acceso a sistemas de información diplomáticos, gubernamentales y militares.

Recientemente, el Secretario General de la OTAN, Jens Stoltenberg expresó que "ha quedado claro que peligrosos ataques pueden ser lanzados en la red y entre redes de computadoras tan fácilmente como es posible en el campo de batalla"[8].

En la medida en que mayor cantidad de información comenzó a ser digitalizada y las comunicaciones pasaron a ser instantáneas, los desafíos de los actores cibernéticos estatales, de organizaciones no gubernamentales y de entes y personas privados pasaron a ser mayores en virtud de la gran cantidad de material al cual se puede tener acceso, tanto de manera lícita o abierta como ilícitamente. En este sentido, mantener la integridad de dicha información a pesar de los intentos de interrumpirla o de atacarla a través de formas digitales de penetración conocidos como virus[9], troyanos, o bien gusanos informáticos que afectan a equipos con el sistema operativo *Windows*, por ser el más conocido, aunque también lo hacen con otros sistemas operativos como *LINUX, DOS, UNIX, MVS, y MACINTOSH,* pasó así a convertirse en otro desafío de seguridad y confiabilidad de la información de todos los usuarios en todas las categorías.

Si bien muchas de estas actividades ilícitas tenían y tienen propósitos delictivos y fraudulentos, no todas pueden encuadrarse en esta categoría. El caso testigo de robo de información sin propósito delictivo ocurrió en la Argentina en 1995, donde un joven ingresó en los archivos secretos del Pentágono vía Londres, usando una línea 0-800 de Telecom. En este caso solo fue un adolescente que incursionaba en la red, sin malas intenciones. Sin embargo, existen ejemplos de robo de información gubernamental y de secretos de empresas y corporaciones llevados a cabo por *hackers* financiados por gobiernos[10], o *hackers* aislados, o *hackers* idealistas, o *hackers* patrióticos. Estos robos de información se consideran ataques porque incursionan en las redes y sistemas de información sin el consentimiento del usuario, y además porque ocasionan resultados o daños concretos[11]. No obstante, las actividades ilícitas no solo se reducen a robar infor-

6 Organization of Security and Cooperation in Europe OSCE, Cyber/ICT Security; Disponible en: http://www.osce.org/secretariat/106324

7 Las principales fuentes en las que se pueden constatar proyectos estratégicos de defensa cibernética son las que siguen: Estados Unidos de Norteamérica, Estrategia Nacional de Ciberseguridad; Brasil: Política de Defensa Cibernética; Colombia: Lineamientos de Política para Ciberseguridad y Ciberdefensa; España: Estrategia de Ciberseguridad Nacional; Francia: Estrategia Nacional de Ciberseguridad; Gran Bretaña: The UK Cyber Security Strategy Protecting and promoting the UK in a digital world.

8 Euronews. Cyberspace is officially a war zone – NATO; Disponible en: http://www.euronews.com/2016/06/15/cyberspace-is-officially-a-war-zone-nato

9 En el glosario que se encuentra al final de la investigación se definen algunos términos del ámbito tecnológico asociados a los ataques cibernéticos.

10 Según fuentes de los Estados Unidos, China podría haber ayudado a Corea del Norte en su ataque a la empresa Sony Pictures, a pesar que la embajada china en Washington señaló que su país no apoya "ciberilegalidades" Disponible en: http://www.telegraph.co.uk/news/worldnews/asia/northkorea/11304283/Sony-hack-China-may-have-helped-North-Korea-US-states.html

11 Según fuentes de los Estados Unidos, China podría haber ayudado a Corea del Norte en su ataque a la empresa Sony Pictures, a pesar que la embajada china en Washington señaló que su país no apoya "ciberilegalidades" Disponible en: http://www.telegraph.co.uk/news/worldnews/asia/northkorea/11304283/Sony-hack-China-may-have-helped-North-Korea-US-states.html

mación, sino que buscan alterar sistemas de funcionamiento cibernético, como ocurrió con el caso del Stuxnet, y *Flame*, gusanos que tienen la capacidad de auto replicarse y de dañar capacidades críticas para las naciones, como son sus programas nucleares.

Frente a este nuevo ambiente, los gobiernos comenzaron a preguntarse qué es lo que podrían esperar del espacio cibernético y cómo conseguirían llegar a defenderse en él. En virtud de ello, las naciones elaboraron estrategias de ciberseguridad y ciberdefensa en casi todo el mundo. La amenaza fue ganando credibilidad en la medida en que con cada vez mayor frecuencia distintas redes tanto civiles como militares eran atacadas por hackers. Fue así que la protección de esas redes pasó a ser un tema de alta prioridad.

En la última década, además de Estados Unidos, países como Brasil[12], Colombia[13], España[14], Francia[15], Gran Bretaña[16], han anunciado sus proyectos estratégicos de defensa cibernética en busca de prevenir y controlar posibles futuros ataques y de incrementar la intensidad informativa y el dinamismo en los sistemas de protección del espacio cibernético. El 21 de abril de 2016, el Primer Ministro de Australia, Honorable Malcolm Turnbull, promulgó la denominada *"AUSTRALIA'S CYBER SECURITY STRATEGY: Enabling innovation, growth & prosperity"*[17]. El hecho es que Estados Unidos, Gran Bretaña, Francia y otros países en su conjunto han gastado billones de dólares en el desarrollo de armas cibernéticas.

Así, Coz Fernández al referirse al liderazgo de Francia en Ciberdefensa, afirma que:

> Francia es uno de los países que mayor evolución ha tenido en la última década en el campo de la Ciberdefensa, pese a no ser uno de los pioneros en esta área, como puedan ser el Reino Unido, Israel, Rusia o Estados Unidos. Desde que Francia publicara su Estrategia Nacional de Ciberseguridad en febrero del año 2011 se ha producido un auténtico terremoto que ha cristalizado en el Programa Nacional de Ciberseguridad que ha hecho público este año 2014. Este programa está dotado presupuestariamente con mil millones de euros[18].

De esta manera, el volumen de gastos -en gran parte realizados con esperanzas de reducir la necesidad de ataques militares más tradicionales- refleja una mayor preocupación sobre una nueva y escasamente probada arma que tiene el potencial de transformar la naturaleza de la guerra; casi de forma similar a lo que sucedió hace poco menos de

---

12 Brasil: Política de Defensa Cibernética.

13 Colombia: Lineamientos de Política para Ciberseguridad y Ciberdefensa.

14 España: Estrategia de Ciberseguridad Nacional.

15 Francia: Estrategia Nacional de Ciberseguridad.

16 Gran Bretaña: The UK Cyber Security Strategy Protecting and promoting the UK in a digital world.

17 Commonwealth of Australia, Department of the Prime Minister and Cabinet, Australia's Cyber Security Strategy, Enabling innovation, growth & prosperity; Disponible en: https://cybersecuritystrategy.dpmc.gov.au/assets/img/PMC-Cyber-Strategy.pdf

18 Coz, Fernández (2014), Francia, un liderazgo en ciberdensa; Disponible en: https://ismsforumspain.wordpress.com/2014/10/21/francia-un-liderazgo-en-ciberdefensa/

un siglo cuando, por primera vez, los aviones fueron utilizados en combate en la Primera Guerra Mundial.

Paralelamente con esto, el ciber espacio fue utilizado por redes sociales como *Facebook, Twitter, Linkedin, Instagram* y otras, cuyo propósito es básicamente relacionar a individuos u organizaciones de acuerdo con algún criterio. La llamada Primavera Árabe en 2011 constituyó, en este sentido, un ejemplo de cómo el avance de Internet y del uso de las redes sociales generó un intercambio continuo y masivo de información, permitiendo así que cientos de personas pudieran organizarse y manifestarse libremente, disponiendo de mecanismos para denunciar los abusos de los gobiernos que, por su parte, no supieron cómo enfrentar a la población y a la opinión pública local e internacional, ya que los tradicionales métodos de censura con los que contaban no pudieron aplicarse a este tipo de lógica comunicacional.

Desde el momento en que las acciones en el espacio cibernético significan enfrentamiento de voluntades, han aparecido nuevos términos como el de *seguridad cibernética, defensa cibernética, agresión cibernética, operaciones cibernéticas* y, desde que el enfrentamiento de voluntades cibernéticas puede causar enormes daños equivalentes o superiores al enfrentamiento físico, el de *guerra cibernética.* Así, la guerra cibernética o guerra "por control remoto" se convirtió en un modo de conflicto que cambia la naturaleza de este fenómeno social. Incorpora nuevas tecnologías y las fuerzas que son necesarias desplegar dejan pocos rastros de su presencia. Ello habilita a quienes deben tomar decisiones de carácter estratégico a aprobar la ejecución de operaciones que difícilmente autorizarían si se emplearan en su lugar medios convencionales.

En 2008, en la Guerra de Georgia, piratas cibernéticos o hackers rusos se habrían dedicado a bloquear o manipular algunas de las principales páginas del gobierno georgiano en Internet. De ser así, este conflicto podría considerarse entonces como la primera guerra cibernética que acompañó a un conflicto bélico a gran escala. Más recientemente, en 2014, al parecer Rusia consideró las operaciones cibernéticas junto con las de las Fuerzas Terrestres y Fuerzas Especiales como operaciones principales a partir del inicio de la campaña contra Ucrania. Para Michael Gordon[19], los expertos que siguen de cerca el éxito de las fuerzas rusas para implementar la política del presidente Vladimir Putin en Crimea y Ucrania oriental "ven que una fuerza militar a la que se desdeñaba y consideraba decadente desde la caída de la Unión Soviética emplea tácticas del siglo XXI que combinan el uso de la guerra cibernética, una enérgica campaña de información y tropas especiales altamente entrenadas, todo destinado a arrebatarle la iniciativa a Occidente".

Debido a estas y otras experiencias, los ataques cibernéticos pasaron a convertirse en una fuente de amenazas en el mundo globalizado porque son capaces de acceder a sistemas de información diplomáticos, gubernamentales y militares. Sin que exista prueba fehaciente, en las elecciones presidenciales de 2016 en Estados Unidos en las que triunfara Donald Trump, el Partido Demócrata acusó a Rusia de haber infiltrado sus computadoras y haber alterado los resultados.

El espacio cibernético posee ciertas características: no tiene límites geográficos como lo puede tener el espacio terrestre o marítimo; es de fácil acceso económico y virtual;

19 Gordon, Michael R. "La estrategia militar innovadora del Kremlin desconcierta a todos"; La Nación, Edición impresa, 23/04/2014 – P. 2

se difuman los conceptos tradicionales de ataque y defensa; puede ser usado para fines loables o, por el contrario, para fines delictivos o para afectar la seguridad de un Estado; es anónimo, y los que incursionan en él pueden ser desde adolescentes en búsqueda de aventuras u organizaciones criminales u organizaciones dependientes de un Estado que busca afectar a otro Estado, o bien hasta organizaciones económicas y financieras que compiten.

También, se desdibuja la diferencia civil - militar puesto que acciones cibernéticas en aspectos civiles pueden afectar las operaciones militares. En todos los casos, individuos y Estados niegan autoría y se escudan en el anonimato. Por otro lado, lo que inicialmente puede ser considerado como independiente de la responsabilidad estatal, tropieza con la norma internacional que responsabiliza a cada Estado del uso de sus medios de informática y telecomunicaciones dentro de sus fronteras.

En el ámbito de responsabilidad de un Estado, la cibernética incluye su administración, el uso de su espacio de telecomunicaciones, las industrias químicas y nucleares, los sistemas de defensa, las actividades de investigación, el abastecimiento de agua, energía y servicios sanitarios, los sistemas de salud, transporte y alimentación, el sistema financiero y tributario y la seguridad interna.

Hasta este momento, las operaciones cibernéticas son consideradas como operaciones complementarias a las tradicionales y, por lo tanto, tomadas en consideración después de que se formulan los planes esquemáticos. Sin embargo, en el caso de la guerra entre Georgia y Rusia, y entre Rusia y Ucrania, las fuerzas convencionales fueron dejadas como operación complementaria en un papel disuasorio y como parte de un Plan de Engaño, en tanto que las operaciones cibernéticas y las Fuerzas Especiales tuvieron la prioridad de las operaciones militares. Es por ello que normalmente las operaciones en el espacio cibernético se deben planificar en el planeamiento deliberado[20], como parte de las campañas en el planeamiento de crisis[21], como respuesta a las crisis y también para las operaciones en curso. Su planificación es imprescindible porque pueden crear efectos simultáneamente en los niveles estratégicos, operacionales y tácticos. Para evitar que dichos efectos se contrapongan, la planificación debe estar completamente integrada a las operaciones conjuntas a nivel del Teatro de Operaciones y a nivel de cada Comando de Componente.

El uso de la cibernética en el ámbito militar puede generar vulnerabilidades inesperadas e introducir costos y riesgos inaceptables y, por ende, el espacio cibernético puede afectar seriamente la dirección, el planeamiento y la ejecución de las operaciones militares.

Este nuevo espacio virtual en su funcionamiento, pero real en su existencia, desde el momento en que el espacio electromagnético usa la capa física del modelo de Interconexión de Sistemas Abiertos, se agrega a los tradicionales de aire, espacio, mar y tierra.

---

20 Se denomina planeamiento deliberado al que responde a las contingencias de empleo del poder militar previstas por el poder político. Es lo que durante la Guerra Fría se denominaba Hipótesis de Conflicto.

21 Se denomina planeamiento de crisis cuando se confirman los supuestos de la contingencia que dio lugar a un planeamiento deliberado. Es lo que durante la Guerra Fría se denominaba Hipótesis de Guerra.

Ocurre que los conocidos como niveles de guerra estratégico, operacional y táctico que piensan en la guerra como un sistema de dirección de niveles estratégicos y planeamiento y ejecución de los niveles operacional y táctico, se difuman. Las acciones cibernéticas militares en cada nivel se superponen y se influencian mutuamente. Los que usan el espacio cibernético en los niveles inferiores no pueden ejercer la iniciativa requerida en cada nivel. Los que usan el espacio cibernético en los niveles estratégicos superiores, inexorablemente afectan los niveles de planeamiento y ejecución. Entonces, si la libertad de acción no se restringe, se puede llegar a situaciones no deseadas por su gravedad; si la libertad de acción se restringe, las reacciones pueden ser tardías.

En suma, un Comandante de un Teatro de Operaciones debe saber cómo incorporar las actividades cibernéticas al método de planeamiento y conocer qué requerir de él en la ejecución de operaciones militares bajo su responsabilidad.

En el nivel regional sudamericano se han llevado a cabo numerosos seminarios y simposios relacionados con el espacio cibernético y la defensa, aunque no específicamente sobre la influencia en el planeamiento y operaciones militares. El espacio cibernético se vislumbra como un escenario de posibles conflictos que pueden ir evolucionando en cuanto a su intensidad hacia enfrentamientos de mayores dimensiones. No obstante, existe un vacío en lo que se refiere a su influencia en las operaciones militares. Probablemente esto ocurra porque los países son renuentes a expresar públicamente sus debilidades cibernéticas, puesto que con ello no harían otra cosa que esparcir sus vulnerabilidades.

Revelar una vulnerabilidad puede significar que un país renuncia a la oportunidad de recolectar inteligencia crucial que podría frustrar un ataque terrorista, detener el robo de propiedad intelectual de ese país o incluso descubrir las vulnerabilidades más peligrosas que están siendo utilizadas por hackers u otros adversarios para explotar sus redes. Es por ello que la divulgación automática no siempre es la opción política más correcta.

A pesar de las graves implicancias no solamente para las fuerzas militares sino para el bienestar de la población civil y los no combatientes producto de las operaciones cibernéticas que se han mencionado aquí a modo de ejemplo, son escasas las investigaciones publicadas acerca de cómo lo planificado por un Comando Conjunto de Ciberdefensa en el nivel estratégico militar puede afectar la integración de operaciones cibernéticas con las operaciones de los comandos geográficos en otros ambientes y en toda la gama de operaciones militares[22].

Por otra parte, la propia experiencia de quienes han participado en la conducción de ejercicios de planeamiento de nivel operacional en los últimos años en la Argentina muestra de manera recurrente que, cuando es necesario planificar una operación simulada en un ejercicio de carácter conjunto, la mayor parte de los cursantes poseen conceptos vagos y/o difusos respecto de las capacidades y limitaciones de las operaciones cibernéticas en un ambiente operacional.

---

22 Prisco, Nicholas E. MAJ, USA The Criticality of Cyber Defense to Operational Commanders; Disponible en: http://www.dtic.mil/dtic/tr/fulltext/u2/a564067.pdf; Leed, Maren; Offensive Cyber Capabilities at the Operational Level; Disponible en: https://www.csis.org/analysis/offensive-cyber-capabilities-operational-level; Farmer, David B. Major, USAF; Do the Principles of War Apply to Cyber War? Disponible en: http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix= html&identifier =ADA522972

Por tales razones, y a fin de cubrir este vacío y la necesidad de contar con información y conocimiento en ese sentido, en esta investigación se indagó sobre el empleo de las capacidades cibernéticas en un Teatro de Operaciones y en el uso de ellas en apoyo a las operaciones de información en el planeamiento y la ejecución de las operaciones militares en el nivel operacional.

El estudio se orientó a los aspectos básicamente militares de lo que ha dado en llamarse la guerra cibernética y dentro de ella, al nivel operacional, lo cual incluye la determinación de las relaciones verticales entre niveles de guerra, y horizontales en el nivel operacional entre componentes del Teatro de Operaciones. No se consideraron explícitamente otros aspectos como la protección de infraestructura crítica, el robo de datos personales, el ciberespionaje industrial y económico, o el uso malicioso de Internet. No obstante, y tal cual se ha mencionado, la consecuencia de un ataque cibernético masivo sobre instalaciones civiles también afecta el empleo del componente militar del poder nacional.

La investigación tuvo un carácter exploratorio, aunque se recurrió a la descripción de las características de los casos seleccionados. Su enfoque fue cualitativo y se sustentó en el análisis bibliográfico de fuentes secundarias.

A lo largo de la investigación se debieron enfrentar numerosos desafíos y limitaciones; el primero de ellos fue la ausencia de bibliografía en español. Este aspecto requirió una intensa búsqueda de información en otros idiomas, con el inconveniente de que ciertas publicaciones omiten aquella que es considerada sensible. Otra limitación fue la carencia de antecedentes relativos al tema.

Finalmente, es conveniente dejar sentado que esta es la primera investigación que se lleva a cabo en este nuevo ámbito, aplicado exclusivamente a las operaciones militares del nivel operacional. En tal sentido, se espera que sirva de base para futuras investigaciones de los cursantes de la Escuela Superior de Guerra Conjunta, que complementen, modifiquen y/o mejoren lo que aquí se expresa.

Como objetivo general de la obra se propuso aportar lineamientos generales respecto de la planificación y el empleo de las operaciones cibernéticas en el nivel operacional y su influencia en el nivel táctico, sin dejar de considerar que, en este tipo de operaciones, es difícil establecer una clara línea divisoria entre lo que es civil y lo que es militar.

En cuanto a los objetivos específicos necesarios para alcanzar el objetivo general, estos se concentraron en:- determinar la forma en que las operaciones cibernéticas afectan al planeamiento y ejecución de las operaciones militares;- establecer el modo en que las decisiones cibernéticas de los niveles de dirección estratégica inciden en el nivel operacional; -vislumbrar de qué manera las fuerzas conjuntas pueden integrar las operaciones en el espacio cibernético para apoyar a las operaciones conjuntas;-determinar el rol de los Comandos de Componente y el de las Fuerzas de Tareas Conjuntas, y diseñar un anexo de operaciones cibernéticas del Plan de Campaña de un Teatro de Operaciones que permita integrar las operaciones cibernéticas de red de computadoras al planeamiento en el nivel operacional utilizando los elementos del arte y diseño operacional.

En lo que hace al orden de los contenidos, la obra se encuentra organizada en seis capítulos. En el primero se definen los conceptos relacionados con la cibernética a los que

se refiere la "Directiva de Política de Defensa Nacional[23]" (DPDN) promulgada por el Decreto 2645/2014 y otros que se consideraron de interés, con el propósito de alcanzar una compresión e interpretación común en tanto que, como se demostró, no existe una definición universalmente aceptada para la mayoría de ellos.

En el segundo capítulo, se compara el estado del arte existente en los países del mundo más avanzados en lo que hace a las estrategias nacionales de defensa y seguridad y se intenta dar cuenta de la forma en que los gobiernos de los países involucrados pretenden lograr un desarrollo cibernético, económico social, institucional y equilibrado entre los estados y la sociedad civil. A modo de ejemplo, se exponen en forma de tabla dos modelos de posibles objetivos estratégicos que podrían ser perfeccionados y servir como base para elaborar una política o estrategia nacional de defensa cibernética en la Argentina[24].

En el capítulo tres se presenta el resultado del estudio de las doctrinas militares en el campo de la ciberdefensa y ciberseguridad derivadas de las estrategias nacionales de defensa cibernética, las cuales han dado lugar a la creación de organismos específicos que contemplan capacidades ofensivas en el espacio cibernético.

En el capítulo cuatro se analiza el espacio cibernético en relación con las operaciones cibernéticas pues las operaciones militares en redes utilizan sistemas de información y telecomunicaciones por donde fluyen las comunicaciones de la gestión del mando y control, las que, por extensión, coadyuvan a la toma de decisiones de diversos niveles de la conducción militar.

En el capítulo cinco, sobre la base del conocimiento adquirido, se determina la forma de integrar las operaciones cibernéticas de red de computadoras al planeamiento en el nivel operacional, utilizando los elementos del arte y diseño operacional.

Finalmente, en el capítulo seis, se describe el empleo de las capacidades cibernéticas en apoyo de las operaciones de información[25], las cuales tienen que ver principalmente con influir en las decisiones y los procesos de toma de decisiones, mientras que, al mismo tiempo, se defienden los procesos de toma de decisiones propios.

---

23 República Argentina. Ministerio de Defensa. Decreto 1514/2009, aprobación de la Política de Defensa Nacional; Disponible en: http://www.ceedcds.org.ar/Srd-LibBL/ARG/DPDN.pdf

24 Hasta el momento, la Argentina carece de una Estrategia Nacional de Seguridad Cibernética, que debiera basarse en una Estrategia Nacional de Seguridad y Defensa, para dar base a una Estrategia Nacional de Defensa Cibernética. Todos estos documentos son inexistentes.

25 El uso de la información puede estar dirigido a informar o a desinformar. Desinformar significa Dar información intencionadamente manipulada al servicio de ciertos fines. Además de la tecnología, interviene la inteligencia humana que hace uso de sus resultados. Pueden consistir en recolectar información, confirmar la veracidad de la información propia, distribuir propaganda o desinformación para socavar la moral, afectar la calidad de la información que obtenga el oponente o negarle la recolección, y otras formas. Vulgarmente, se identifica a las Operaciones de Información únicamente a actividades electrónicas de escucha, pero es un concepto muy incompleto.

CAPÍTULO 1

TÉRMINOS Y DEFINICIONES

Introducción

Según Luis Feliú Ortega[26], hasta hace algunos años no existía un problema respecto de las definiciones "porque se seguía el método cartesiano y por la influencia de los sistemas francés y alemán cuyos idiomas son muy precisos. Sin embargo, en la actualidad, la influencia de las doctrinas anglosajonas muy poco proclives a preocuparse por la precisión en el lenguaje y la tendencia a utilizar la ambigüedad y los eufemismos en la utilización de determinados conceptos, han hecho que exista bastante confusión".

Esto no es simplemente una cuestión de palabras, pues cuando se trata de asignar competencias o misiones y tareas en el campo de la cibernética a las Fuerzas Armadas, esta confusión es aún mayor. Es obvio que debe existir una comprensión común de términos para poder entenderse. Esta comprensión común se vuelca en la doctrina[27], que es lo que se enseña.

En la actualidad, no existen definiciones comunes para expresiones relacionadas con la cibernética, ni siquiera en contextos regionales, lo cual sin duda dificulta la cooperación entre Estados en temas de defensa. A pesar de la prevalencia en los medios y en las declaraciones de organizaciones nacionales e internacionales, los términos parecieran significar cosas distintas y esto resulta un obstáculo cuando los países -o los distintos organismos dentro de un mismo país- necesitan compartir información para conocer si se trata de un ataque, de una intrusión o de un aficionado y hacia dónde está dirigido. La causa a la que se puede atribuir esta miríada de definiciones reside en el diferente marco legal y regulatorio de cada país sobre el espacio cibernético y también a las dificultades en su traducción.

26 Feliú, Ortega Luis, "La Confusa Terminología de la Seguridad y la Defensa, Instituto Español de Estudios Estratégicos, "Documento de Opinión" 06/2012; Disponible en: http://www.ieee.es/Galerias/fichero/docs_opinion/2012/DIEEEO06-2012_ConfusaTerminologia_Seg.Def._GB_Feliu.pdf

27 Doctrina: Conjunto de principios generales que se fijan en un campo determinado para la correspondiente educación de sus componentes y para la orientación de la acción. Estado Mayor Conjunto de las Fuerzas Armadas, Glosario de Términos de Empleo Militar para la Acción Militar Conjunta PC 10-03, Proyecto 2013, P. 106.

Para darse cuenta de la importancia de una terminología común, nada mejor que reproducir este párrafo del libro de Singer y Friedman *Cybersecurity and Cyberwar*[28]:

> Transcurrió un largo tiempo para reunir a los dos grupos, pero finalmente los directivos americanos y chinos se juntaron alrededor de la misma mesa. Los asuntos importantes en la agenda de las dos superpotencias iban desde asuntos de comercio y finanzas a las preocupaciones emergentes de la ciberseguridad. Pero finalmente cuando las discusiones comenzaron, la delegación china estaba desconcertada. Los representantes de Estados Unidos hablaron acerca de la importancia del *"engagement"*. El traductor chino no estaba seguro si los americanos estaban haciendo una propuesta de casamiento, o si querían discutir acerca de un intercambio de disparos, nada de lo cual parecía apropiado para una reunión de diplomáticos... Tratar de hablar acerca de un nuevo asunto puede asimilarse un poco a un viaje en tierra extranjera. Nuevas discusiones requieren enteramente un nuevo vocabulario y un encuadramiento solamente para entender lo que está pasando. Puede ser más complejo en el dominio de los asuntos ciber, en tanto los tópicos se mezclan en grado sumo con asuntos técnicos complicados y con amplios conceptos en los cuales aún los términos más básicos pueden ser equiparados a significados pre- existentes.

Otra evidencia de ello es que mientras se realizaba un Seminario Regional de Ciberdefensa en el ámbito de la Unión de Naciones Suramericanas (UNASUR) donde "se expusieron temas en torno a las infraestructuras críticas y seguridad de la información, a los ecosistemas de computación en la nube, a la seguridad de las comunicaciones y a las tecnologías de la información y de las comunicaciones, entre otros", se conformó, cerrada al público, la tercera reunión del Grupo de Trabajo de Ciberdefensa, en el marco del Consejo de Defensa Suramericano. En dicha reunión se determinó, entre otras cosas, la necesidad de *"Profundizar y sistematizar la reflexión sobre definiciones conceptuales de ciberdefensa y ciberseguridad (Declaración de Cartagena del Consejo de Defensa Suramericano, 2014)"* [29]

Casi un año más tarde, en abril de 2015, durante el segundo día del II Simposio Internacional en Seguridad y Defensa "Espacio cibernético, Ciberseguridad y Ciberdefensa" llevado a cabo en la Escuela de Guerra Naval de Perú, el Doctor Kevin Newmeyer señaló: "las definiciones en cibernética continúan evolucionando; sin embargo, es necesario establecer una línea base por lo que se debe definir Espacio cibernético, Ciberseguridad y Ciberdefensa".

Ese mismo mes, se celebró en Holanda la Conferencia Global 2015 sobre el Espacio Cibernético, con la presencia de casi dos mil funcionarios de gobiernos, académicos, representantes de la industria y otros participantes. Al concluir dicha conferencia, Aus-

---

28 Singer P. and Friedman Allan, Cybersecurity and Cyberwar, Oxford University Press, Library of the Congress, 2014, P. 67; Disponible en: https://news.asis.io/sites/default/files/Cybersecurity_and_Cyberwar.pdf

29 Justribó, Candela "Ciberdefensa: Una visión desde la UNASUR", VII Congreso del Instituto de Relaciones Internacionales, La Plata, 26 al 28 de noviembre de 2014; Disponible en: http://sedici.unlp.edu.ar/bitstream/handle/10915/44716/Documento_completo.pdf?sequence=1

tralia[30] sostuvo que "el panorama internacional era demasiado "prematuro" [sic] para alcanzar un acuerdo internacional integral respecto de la forma de gobernar internacionalmente la seguridad en el espacio cibernético. Con desacuerdos sobre incluso la terminología cibernética más básica, sin mencionar las normas básicas que rigen las actividades del estado en el espacio cibernético, existe una necesidad de concentrarse en aspectos clave y orientar los esfuerzos hacia la creación de normas".

Por otra parte, dentro del sector privado (que incluye la industria de Internet), medios de comunicación e incluso aquellos relacionados con la ciberdefensa y la ciberseguridad, utilizan términos diferentes para describir lo mismo - ya sea un evento intrascendente o una amenaza inminente. Por el contrario, representantes de estos sectores pueden utilizar el mismo término para describir cosas muy diferentes.

En este capítulo, en una primera parte, se exponen las distintas acepciones y definiciones que poseen los conceptos relacionados con la cibernética a los que se refiere la "Directiva de Política de Defensa Nacional" (DPDN).

En una segunda parte, se realiza una breve descripción de los términos: Internet y *World Wide Web (www)*, los cuales suelen utilizarse indistintamente, a pesar de sus diferencias; asimismo se presentan algunas posturas sobre Gobernanza de Internet.

Análisis de los distintos términos contemplados en la Directiva de Política de Defensa Nacional

En la Directiva de Política de Defensa Nacional[31] promulgada por el Decreto 2645/2014, se mencionan determinados términos relacionados con la guerra cibernética tales como ciberseguridad, ciberdefensa, ataque cibernético, etc. para los cuales, como ya se dijo, no hay definiciones universalmente aceptadas pero que, para el propósito de este libro se hacen necesario comprender.

De lo investigado, surge que las bases de dicha Directiva, en lo que respecta a los términos que ella contempla, se encuentran en un documento presentado en diciembre de 2012, en el VI Congreso de Relaciones Internacionales organizado por el Instituto de Relaciones Internacionales (IRI) de la Universidad Nacional de La Plata (UNLP) denominado: "El ciberespacio y sus implicancias en la defensa nacional. Aproximaciones al caso argentino".[32]

El propósito de este documento fue separar la seguridad cibernética nacional de la defensa cibernética nacional, en vez de integrarlas. Asimismo, buscó dar un marco racional al uso militar de la cibernética únicamente ante agresiones externas de otros estados, como si en el espacio cibernético se pudiera saber con precisión desde el inicio, el origen, la atribución, el propósito y el destino y efectos de un ataque cibernético. Ade-

30 ASPI, Ausecurity and Cyberwarstralian Strategic Policy Institute, Tallinn2.0 Cyberspace and the law, artículo de Klée Aiken y Jessica Woodall, página web The Strategist, de fecha 14 Mayo 2015; Disponible en: http://www.aspistrategist.org.au/tallinn-2-0-cyberspace-and-the-law/

31 República Argentina. Ministerio de Defensa. Decreto 2645/2014. Directiva de Política de Defensa Nacional. Apruébase actualización; Disponible en: http://www.infoleg.gov.ar/infolegInternet/anexos/240000-244999/240966/norma.htm

32 Eissa, Sergio G., Gastaldi, Sol, Poczynok, Iván y Zacarías Di Tullio, María Elina, El ciberespacio y sus implicancias en la defensa nacional. Aproximaciones al caso argentino; Disponible en: http://sedici.unlp.edu.ar/bitstream/handle/10915/40210/Documento_completo.pdf?sequence=1

más, como por un lado sostiene que determinar la atribución es casi un imposible, restringe el accionar de la defensa cibernética activa ante el riesgo de encontrarse con una agresión militar de un servidor dentro del país.

Aunque útil como construcción intelectual tradicional, este concepto ideológico divisorio de seguridad versus defensa es arcaico en su implementación, dadas las características del espacio cibernético y más aún luego de la Guerra Fría[33]. De aquí que se entiende que este documento de la UNLP estuvo basado en supuestos y definiciones no técnicas que en general fueron y -aún podrían ser hoy - tomadas por válidas, lo que hace suponer falacias de autoridad[34]. Según este documento, como la ley argentina vigente desde 1988 prohíbe cualquiera otra participación militar en el espacio cibernético, debe propugnarse y mantenerse tal diferencia.

Además, no se definen allí áreas de responsabilidad y, por lo tanto, no posibilitaría la aplicación de una ley porque no hay ejercicio soberano de un país si no se asume una jurisdicción. Por lo expresado, esta postura académica carecería de sustento por su definición sobre ciberespacio ya que no se enfoca en la causa-efecto que lo define y así entendido, no se puede ejercer una salvaguarda de derechos de un espacio que no reconoce, porque al no hacerlo -como ya se mencionó-, no estaría determinando su jurisdicción. Por lo tanto, no habría ley nacional ni internacional que se le pueda aplicar. Así, todo argumento basado en el derecho anterior a la aceptación de la existencia del espacio cibernético carece de sustento.

Vinculado con lo anterior, aunque con una postura más bien contraria a lo expresado en ese documento de la UNLP, la OTAN, como también gran parte de los países del mundo, han incorporado al día de hoy el concepto de espacio cibernético separado de los espacios tradicionales y con implicancias militares, en razón de los daños que su mal uso puede causar.

Cibernética

La Directiva de Política de Defensa Nacional establece que "Los usos militares de las novedosas tecnologías asociadas a la robótica, cibernética, sensores remotos, entre otros desarrollos en materia de ciencia y tecnología, han impulsado nuevas formas de librar la guerra que exhiben un salto cualitativo hacia un nuevo paradigma tecnológico".

De manera corriente suele aparecer un nuevo término o bien uno viejo obtiene un significado nuevo y espontáneamente se habla de él en todas partes. En los últimos años (décadas, podría decirse), la palabra "cibernética" se ha agregado a una larga lista de palabras para crear nuevos términos.

A pesar del tiempo transcurrido desde que se acuñara por primera vez, no es fácil explicar qué es la cibernética y cualquier definición que se ensaye seguramente ha de resultar imprecisa e insuficiente, pues generalmente dentro de la cibernética pueden distinguirse varios puntos de vista diferentes.

---

33 Ballesteros Miguel Ángel, Hacia una Estrategia de Seguridad Nacional, Instituto de Estudios Estratégicos de España, Madrid, 2016 Cap. 2, Pág. 60; Disponible en: http://www.ieee.es/Galerias/fichero/OtrasPublicaciones/Nacional/2016/MABM_ESN.pdf

34 Una falacia de autoridad supone dar algo por verdadero porque se supone que quien lo dice es una autoridad en el tema.

Para el Diccionario de la Real Academia Española ciber- Del ingl. *cyber-*, acort. de *cybernetic* 'cibernético'. *"1. elem. compos. Indica relación con redes informáticas. Ciberespacio, cibernauta". Para el mismo diccionario, cibernética (del fr. cybernétique, este del ingl. cybernetics, y este del gr. κυβερνητική, arte de gobernar una nave) es el "estudio de las analogías entre los sistemas de control y comunicación de los seres vivos y los de las máquinas; y en particular, el de las aplicaciones de los mecanismos de regulación biológica a la tecnología".*

Para Stuart Umpleby y Eric Dent[35], el término aparece por primera vez en 1948 como título del libro *"Cybernetics"* escrito por Norbert Wiener, profesor de Matemáticas del Instituto de Tecnología de Massachusetts, que a su vez lleva un subtítulo que busca aclarar el alcance del ensayo: "Control y Comunicaciones en los Animales y las Máquinas".

Para los autores, Weiner propuso la noción de una segunda revolución industrial. "La primera revolución industrial se produjo cuando las máquinas comenzaron a reemplazar la energía humana y la segunda cuando las máquinas empezaron a reemplazar la capacidad humana para procesar información y tomar decisiones".

Otra acepción de la cibernética guarda relación con la electrónica. Según ella, durante la guerra de Vietnam, la investigación en los campus universitarios, apoyados por el Departamento de Defensa, comenzó a ser un tanto controversial. Un resultado de dicha discusión fue la denominada enmienda Mansfield, según la cual, los investigadores financiados por dicho organismo tenían que explicar la relevancia de sus investigaciones con respecto a la misión de las Fuerzas Armadas. Es así como los investigadores en inteligencia artificial, como una forma de justificar la financiación, crearon la idea de que en un futuro las batallas se librarían utilizando robots o sensores electrónicos. De ahí la razón por la que, durante la guerra de Vietnam, la cibernética contribuyó a la idea de un "campo de batalla electrónico"[36].

Por último, se encuentra el término "cibernética de segundo orden" que fuera acuñado en 1970 por Heinz Von Foerster en su trabajo titulado *"Cybernetics of cybernetics"*, que se ocupa del observador como parte de lo observado y se refiere a los sistemas que son capaces de modificar su objetivo o finalidad (o su camino) por sí mismos, sin necesidad de ser guiados por alguien o algo desde fuera del sistema. Es una ciencia de acción en la que los mecanismos de comunicación y control permiten que el sistema reoriente o replantee continuamente su camino para alcanzar su objetivo primario[37].

Quienes adhieren a esta última acepción están más interesados en cognición, adaptación y comprensión, temas sobre los que no están tan preocupados la mayoría de los especialistas en sistemas, a pesar de que han comenzado a adoptar una posición epistemológica más constructivista.

Para el Profesor del Instituto Tecnológico Buenos Aires, Roberto Bloch[38], "la Cibernéti-

---

35 Citado por Stuart A. Umpleby y Eric B. Dent, The Origins and Purposes of Several Traditions in Systems Theory and Cybernetics; Cybernetics and Systems: An International Journal, 30:79-103, 1999; Disponible en: http://www.gwu.edu/~umpleby/recent_papers/1998_origins_purposes_several_traditions_systems_theory_cybernetic_1.htm

36 Ibidem.

37 Nemiche, Mohamed; "Un Modelo Sistémico de Evolución Social Dual" Disponible en: http://www.uv.es/nemiche/thesis.pdf

38 Bloch, Roberto, "Cibernética"; Disponible en: http://uprociber.blogspot.com.ar/2008/04/cibernetica.html .

ca constituye una disciplina que trata de realizar una conjunción de los datos suministrados por las matemáticas, la neurología, la mecánica electrónica, etc., con el fin de lograr un dispositivo capaz de realizar elevadas y complejas funciones similares al pensamiento".

Por tal razón, para la cibermedicina, la cibernética tiene dos desarrollos teóricos principales que son la Teoría de la Información y la Teoría de la Robótica. La primera es la rama más relacionada con el pensamiento, mientras que la otra se relaciona más con el desarrollo de partes funcionales; por ejemplo: prótesis auditivas, piernas ortopédicas, y otros objetos similares.

En función de ello, la Agencia de Proyectos Avanzados de Investigación de Defensa (DARPA)[39], lleva adelante el desarrollo de prótesis que suplementan cuerpos dañados o perdidos con la integración de un artificio mecánico o se realizan implantes biónicos que permiten que modelos de órganos o partes del cuerpo sean capaces de imitar la función original de una manera más exacta, con la finalidad de ayudar a los veteranos de guerra con miembros amputados[40].

En consonancia con ello, Alfonso Orciuoli[41] indica que la cibernética debe ser entendida como "una ciencia interdisciplinaria que incluye la psicología, la inteligencia artificial, la economía, la ingeniería de sistemas de control de organismos vivos, máquinas y organizaciones, los sistemas de comunicaciones, la que, al ponerse en movimiento, la información se transforma en una actuación o resultado deseado."

Desde un punto de vista militar, para Van Creveld, "la cibernética y las computadoras trajeron algo más que cambios en la administración, la logística, las comunicaciones, la inteligencia y las operaciones, también ayudó a que un nuevo conjunto de personas, personas que pensaban la guerra – y que, por lo tanto, la planeaban, preparaban, libraban y evaluaban – pudieran hacerse cargo de ello con la ayuda de nuevos criterios y desde un punto de vista totalmente novedoso[42]."

Para Brett Williams[43] la palabra "cyber" "no debe ser usada como verbo ni debe emplearse como un sustantivo que puede valerse por sí mismo". "Cibernética no implica solamente un ataque, ni debe conducir inmediatamente a asumir que la actividad en el espacio cibernético es toda sobre espionaje, delincuencia o una invasión al derecho a la intimidad".

La cibernética no pregunta "¿Qué es esto?" sino "¿Qué hace?" y "¿Qué puede hacer?" Debido a que muchos sistemas en el mundo, en la vida y en el mundo social y tecnológico

---

39 Agencia del Departamento de Defensa de Estados Unidos responsable del desarrollo de nuevas tecnologías para uso militar. Fue creada en el año 1958 como consecuencia tecnológica de la llamada Guerra Fría y de la que surgieron los fundamentos de ARPANET, red que dio origen a Internet.

40 Para Arthur House, "Hemos entrado en la edad de los cyborg, u organismo cibernético: un ser viviente natural y artificial. Retinas artificiales e implantes cocleares (que conectan directamente al cerebro a través del sistema del nervio auditivo) permiten la restauración de la vista a los ciegos y del oído a los sordos. Implantes de cerebro, conocidos como "marcapasos cerebral", alivian los síntomas de los enfermos de Parkinson en todo el mundo"; Disponible en: http://s.telegraph.co.uk/graphics/projects/the-future-isandroid/

41 Orciuoli, Alfonso, citado por Stel, Enrique en "Guerra Cibernética" Círculo Militar, 1ra. Edición, 2005, Buenos Aires, Argenrtina, P. 14

42 Van Creveld Martin; "Technology and War: From 2000 B.C. to the Present" Ed. Simon and Schuster, 11 May. 2010; P. 246.

43 Williams, Brett T.; Cyberspace: What is it, where is it and who cares? Disponible en: http://www.armedforcesjournal.com/cyberspace-what-is-it-where-is-it-and-who-cares/

pueden ser entendidos de esta manera, la cibernética atraviesa varias fronteras disciplinarias tradicionales. Los conceptos que los cibernéticos desarrollan forman así un lenguaje más allá de lo disciplinario, por el que mejor se puede comprender y modificar el mundo.

La tecnología cibernética ha impulsado grandes progresos y ha hecho mucho más eficaz al mundo moderno. Gracias a la cibernética, existe información médica en abundancia y su accesibilidad no tiene paralelismo en la historia de la civilización. El uso de computadoras e Internet para diagnósticos y evaluación iniciales, para decidir tratamientos, realizar investigaciones, prevención de enfermedades y - sobre todo – mejorar la vida de los pacientes, podría decirse que casi no tiene límites.

También, gracias a las computadoras y a Internet, actualmente se puede operar y proyectar el poder en y desde el espacio cibernético para influir en el comportamiento de las personas o el curso de los acontecimientos. Merced a ella, ha comenzado a librarse una nueva forma de guerra, en la que aviones no tripulados o drones realizan misiones mientras su piloto se encuentra a miles de kilómetros de distancia, se puede controlar el sistema radar enemigo para crear información falsa en las pantallas y así desviar su atención hacia blancos inexistentes o identificar a un terrorista a miles de kilómetros de distancia por medio de la biometría.

Espacio cibernético

¿Qué es el espacio cibernético? Uno de los primeros escollos con que se tropieza al tratar este tema es la diversidad y variedad de las definiciones.

> *"No es un camión. Es una serie de tubos".* Esto es cómo célebremente el último Senador de Alaska Ted Stevens explicó al ciberespacio durante una audiencia del Congreso en 2006. Mientras que es fácil burlarse de la noción del anciano senador respecto del envío de cartas electrónicas a través de tubos, la realidad es que puede ser difícil definir ideas y los términos en asuntos cibernéticos. Los "tubos" de Stevens es realmente una forma de expresar la idea de "ductos", una analogía que utilizan los expertos en la materia para describir las conexiones de datos[44].

En relación con este concepto de espacio cibernético, el Decreto 2645/2014 señala:

> Otro aspecto asociado al nuevo paradigma tecnológico y a las tecnologías de la información es la importancia que está adquiriendo el espacio cibernético para el desarrollo de las operaciones militares. La dimensión ciberespacial, sin locación física específica propia, genera replanteos sobre las tradicionales categorías con las que se aborda la "guerra real" y exige, por la dinámica propia de la innovación tecnológica, una rápida adaptación para los Sistemas de Defensa respecto de sus componentes. En las últimas décadas, muchos países vienen reorientando esfuerzos y recursos para resguardar no sólo los espacios tradicionales (terrestre, marítimo y aeroespacial),

44 Singer P. W. and Friedman Allan, Cybersecurity and Cyberwar, Op. Cit. P. 13

sino también al ciberespacial. Este no constituye un "espacio en sí mismo", sino una dimensión que atraviesa a dichos espacios físicos, con medios y reglas propias[45].

Eissa y otros[46], refiriéndose al espacio cibernético señalan:

> La globalidad como fenómeno reviste importancia por su impacto en el espacio físico, ya que es allí donde se manifiesta la vida social de los hombres. En consecuencia, se puede afirmar que este nuevo ámbito de circulación de información no constituye un espacio en sí mismo, sino más bien una dimensión superpuesta, que atraviesa a los espacios físicos tradicionales. En esta misma dirección, Sheldon indica que los dominios clásicos generan efectos estratégicos en cada uno de los otros, pero el ciberpoder genera efectos en todos los espacios de forma absoluta y simultánea (Sheldon, 2011)[47]. Si bien esta distinción es de carácter analítico, resulta de vital importancia para comprender las implicancias del ciberespacio en el ámbito de la defensa, ya que las operaciones virtuales –entendidas como operaciones de información– resultan de interés para los estados por su capacidad de producir alteraciones y/o modificaciones en el mundo físico.

Para Daniel Sierra[48], la pregunta es obligada, ¿Qué es distinto en el espacio cibernético con respecto al mundo tangible? Para él, el espacio cibernético "es el conjunto de medios y procedimientos basados en las Tecnologías de la Información y la Comunicación (TIC) configurados para la prestación de servicios. Está constituido por hardware, software, Internet, servicios de información y sistemas de control que garantizan la provisión de aquellos servicios esenciales para la actividad socioeconómica de cualquier estado, en especial aquellos ligados a sus infraestructuras críticas". De esta forma, se infiere que el espacio cibernético no es solo Internet, ya que Internet forma parte del espacio cibernético. Internet es comunicaciones y comunicaciones es solamente el escenario cibernético.

Para Feliú Ortega "El espacio cibernético es mucho más que Internet[49], más que los mismos sistemas y equipos, el hardware y el software e incluso que los propios usuarios, es un nuevo espacio, con sus propias leyes físicas que, a diferencia de los demás espacios, ha sido creado por el hombre para su servicio".

---

45 La redacción de este párrafo es deficiente porque no se ha mencionado el espacio, que es otro ámbito tradicional, además se lo ha unido al espacio cibernético. O sea que, en vez de decir aeroespacial, se dice ciberespacial dando a entender erróneamente que el ciberespacio es transversal, cuando en realidad es vertical y transversal, como lo fue la aviación en su momento. El subrayado es propio.

46 Eissa, Sergio G., Gastaldi, Sol, Poczynok, Iván y Zacarías Di Tullio, María Elina, Op. Cit.

47 Sheldon, John (2011) "Deciphering Cyberpower.Strategic Purpose in Peace and War", en Strategic Studies Quarterly, Summer Edition; Disponible en: http://www.airuniversity.af.mil/SSQ/

48 Sierra, Daniel; Las dos caras de la tecnología Opinion Ciberelcano; Informe mensual de ciberseguridad; abril 2015 / Nº 2; P. 16.

49 Feliú, Ortega Luis, El espacio cibernético nuevo escenario de confrontación, Cuadernos del CESEDEN, febrero de 2012, Páginas 42 y 43; Disponible en: http://www.defensa.gob.es/ceseden/Galerias/destacados/publicaciones/monografias/ficheros/126_EL_ESPACIO CIBERNÉTICO_NUEVO_ESCENARIO_DE_CONFRONTACION.pdf

El autor[50] además señala que "El Espacio cibernético es lo que se denomina un *Global Common*, entendiendo por tal aquel entorno en los que ninguna persona o estado puede tener su propiedad o control exclusivo pero que son básicos para el desenvolvimiento de la vida de las personas y de las colectividades. Son *global commons* el mar, el espacio extraterrestre, el espacio electromagnético y por supuesto el espacio cibernético que, sin embargo, posee una serie de características diferenciales del resto de los espacios".

Para Rain Ottis y Peeter Lorents[51] "es un conjunto de sistemas de información interconectados dependientes del tiempo[52] y los usuarios humanos que interactúan con estos sistemas".

De manera similar, el Dr. Roberto Uzal[53] de la Universidad de San Luis, Argentina, lo define como "la dimensión generada durante el tiempo de interconexión e interoperabilidad de redes, sistemas, equipos y personal relacionados con los sistemas informáticos cualesquiera sean estos y las telecomunicaciones que los vinculan".

Héctor Flores (coronel retirado del Ejército Argentino)[54], en un libro editado por el Estado Mayor Conjunto de las Fuerzas Armadas de la República Argentina, señala que es "el ámbito electrónico formado por ordenadores en redes y la infraestructura asociada a los mismos."

Para la República Federativa del Brasil[55], "El Ciberespacio es una de las cinco áreas operacionales[56] que penetra todas las demás las cuales son: la tierra, el mar, aire y espacio, que son interdependientes. Las actividades en el ciberespacio pueden crear libertad de acción para las actividades en otras áreas, así como actividades en otros dominios y también crean efectos dentro y a través del ciberespacio. El objetivo central de la integración de dominios es la capacidad de aprovechar las capacidades de múltiples dominios para crear efectos únicos y a menudo decisivos".

Para el Reino de España[57] "es el nombre por el que se designa al dominio global y dinámico compuesto por las infraestructuras de tecnología de la información – incluida Internet–, las redes y los sistemas de información y de telecomunicaciones".

---

50 Ibídem P. 44

51 Rain, Ottis, Lorents, Peeter, "Cyberspace: Definition and Implications", Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia, 2012.

52 La inclusión del factor tiempo en la definición, se debe a que, en el espacio cibernético, los usuarios, los nodos y las conexiones pueden aparecer y desaparecer, y la información se transforma con el correr del tiempo. Comparado con otros sistemas dependientes del tiempo, se observa, que, en el espacio cibernético, pueden ocurrir cambios radicales en muy poco tiempo. Por ejemplo, un código maligno puede replicar, infectar y desactivar de manera efectiva una gran parte de una red global en cuestión de segundos o minutos.

53 Uzal Roberto, Ciberdefensa-Ciberseguridad: Riesgos y Amenazas, conferencia pronunciada en el Consejo Argentino para las Relaciones Internacionales, CARI noviembre 2013

54 Flores, Héctor, "Los ámbitos no terrestres en la guerra futura: espacio cibernético". En Flores, H. (comp.) Los ámbitos no terrestres de la guerra futura: espacio cibernético- aeroespacio, Estado Mayor Conjunto de las Fuerzas Armadas- Gabinete de Estrategia Militar, Buenos Aires, 2012

55 Doutrina Militar de Defesa Cibernética - MD31- M-07 (1ª Edição /2014) de la República Federativa de Brasil. P. 18/36; Disponible en: http://www.defesa.gov.br/arquivos/legislacao/emcfa/publicacoes/doutrina/md31_m_07_defesa_cibernetica_1_2014.pdf.

56 Se debe ser específico con la palabra "operacional", que es un nivel de guerra. Seguramente se quiso decir "operaciones" (el error puede deberse a problemas de interpretación en la traducción del idioma al español).

57 Reino de España, Estrategia de Ciberseguridad Nacional, 2013 P. 9 Disponible en: www.dsn.gob.es/es/file/146/download?token=Kl839vHG

El Estado Mayor de la Defensa de España en su Concepto de Ciberdefensa Militar lo define como "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".

Para el Reino Unido de Gran Bretaña[58] "es un dominio interactivo compuesto por redes digitales que se utiliza para almacenar, modificar y comunicar información. Incluye Internet, pero también los sistemas de información que soportan empresas, infraestructura y servicios. Las redes digitales actualmente sostienen el suministro de electricidad y agua a los hogares, ayudan a organizar la entrega de alimentos y otros bienes a los comercios y actúan como una herramienta esencial para las empresas en el Reino Unido. Su alcance se incrementa en la medida en que se conectan los electrodomésticos, televisores y consolas de juegos".

En un documento de reciente publicación denominado *Cyber Primer*[59], el Reino Unido luego de aclarar que dada la inexistencia de una definición comúnmente aceptada, define al espacio cibernético, según su propia doctrina como "Un entorno operativo que consiste en la red interdependiente de las infraestructuras de tecnología digital (incluyendo plataformas, Internet, redes de telecomunicaciones, sistemas informáticos, así como procesadores y controladores) y los datos en ella que abarcan los dominios físicos, virtuales y cognitivos".

Otra posible definición es: "un ámbito caracterizado por el uso de la electrónica y el espectro electromagnético para almacenar, modificar e intercambiar datos a través de los sistemas en red y la infraestructura física asociada. El espacio cibernético se puede considerar como la interconexión de los seres humanos a través de los ordenadores y las telecomunicaciones, sin tener en cuenta la dimensión física"[60].

En 2011, los Estados Unidos, "anunciaron que ellos consideraban el espacio cibernético como un dominio operacional de la guerra y que respondería a los ataques hostiles en el espacio cibernético como lo haría ante cualquier otra amenaza"[61].

Para el General Brett Williams[62], Director de Operaciones del *US CyberCommand,* es simplemente:

> El dominio artificial creado al conectar todos los ordenadores, conmutadores, enrutadores, cables de fibra óptica, dispositivos inalámbricos, satélites y otros componentes que nos permiten mover grandes cantidades de datos a velocidades muy rápidas. Al igual que en los dominios físicos, terrestre, marítimo, aéreo y espacial, en

---

58 UK Cabinet Office, The UK Cyber Security Strategy Protecting and promoting the UK in a digital world Disponible en: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/516331/UK_Cyber_Security_Strategy_Annual_Report_2016.pdf

59 Ministry of Defense, Development, Concepts and Doctrine Centre, Cyber Primer, (2nd Edition), 2016.

60 Definición extraída del Glosario de Términos Informáticos, Whatis Glossary; Disponible en: http://whatis.techtarget.com/.

61 Voanews; "NATO Likely to Designate Cyber as Operational Domain of War" Disponible en: http://www.voanews.com/a/nato-likely-to-designate-cyber-as-operational-domain-of-war/3356909.html.

62 Williams Brett T, The Joint Force Commander's Guide to Cyberspace Operations, Joint Force Quarterly 73, 2nd Quarter 2014, P. 14; Disponible en: http://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-73/jfq-73_12-19_Williams.pdf

> el espacio cibernético llevamos a cabo una variedad de actividades en beneficio de individuos, gobiernos y entidades comerciales. La diferencia clave entre los dominios físicos y el espacio cibernético es que el espacio cibernético es artificial y cambiante. Esta característica ofrece tanto oportunidades como riesgos.

El mismo autor, en cuanto al uso militar del espacio cibernético señala que, "si se concentra la atención en el nivel operacional de la guerra, se encuentra que las operaciones en el espacio cibernético son bastante similares a las operaciones que se llevan a cabo en los otros ámbitos". El espacio cibernético es un espacio operacional, como es el mar, el aire, la tierra y el espacio. Si el nivel operacional busca colocarse en la mejor posición para llevar a cabo los enfrentamientos, al espacio cibernético le cabe un papel importante en tal acción.

En este punto es necesario adentrarse en nueva terminología. Se entiende por dominio a los cinco ambientes donde se desarrollan los conflictos armados, a saber: aire, mar, tierra, espacio y cibernético. De estos dominios, cuatro de ellos son reales, y el quinto es virtual. El cibernético, al igual que los otros cuatro dominios físicos, tiene características distintivas que requieren una doctrina especializada, una política de empleo, recursos estandarizados entre las Fuerzas Armadas y expertos en el tema. Debido a su reciente aparición, el espacio cibernético es más dificultoso de comprender porque no es fácil adentrarse en un espacio virtual, pero si se habla del nivel operacional de guerra, se encuentra que tiene muchísimas similitudes con los otros dominios.

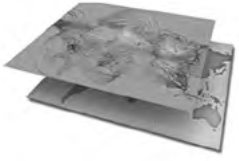
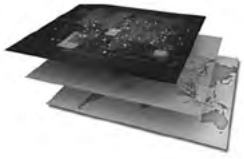
> En lo único que hay que cuidarse es en las analogías erróneas que por simplistas pueden llevar a error. El primer impulso al comparar dominios es equiparar al espacio con el cibernético, ya que tienen la característica común de no tener fronteras. Sin embargo, esta analogía es simplista, porque existen soluciones técnicas que permiten atenuar las limitaciones que surgen de la falta de límites geográficos en el espacio cibernético, señala Williams[63].

Sin embargo, hay otras características que permiten asociar más al espacio cibernético con los tres dominios territoriales. Por ejemplo, en el espacio cibernético pueden apreciarse efectos tanto en el nivel estratégico, como en el operacional y en el táctico, lo que no ocurre en el dominio espacio. También, en el espacio cibernético convergen actores civiles internos e internacionales, comerciales y gubernamentales, los que van a influenciar a las operaciones cibernéticas militares. Luego, tal como ocurre con los dominios territoriales, habrá que preocuparse del fratricidio, de los no combatientes, de los daños colaterales, de la proporcionalidad, de la discriminación y de las reglas de empeñamiento. Otra similitud más del dominio cibernético es que al igual que los territoriales, los combatientes pueden introducir nuevas capacidades, métodos, técnicas y procedimientos mucho más rápido que en el espacio, y en el espacio cibernético ello ocurre de manera más rápida que en cualquier otro dominio.

---

63 Ibidem.

FIGURA 1: EL ESPACIO CIBERNÉTICO EN CAPAS[64]

Capa física	Capa lógica	Capa social
Componentes geográficos  Componentes de red física 	Componentes de red lógica 	Componentes de persona  Componentes de Ciber persona 

El espacio cibernético también puede ser representado en términos de capas[65]: la física, la lógica y la social, cada una de las cuales, como se verá en el capítulo 5, representa un nivel en el cual se podrán conducir operaciones cibernéticas.

La capa física es el medio por donde transitan los datos. El componente geográfico es la ubicación, ya sea en tierra, en el aire, el mar o el espacio, donde se encuentran los elementos de las redes. Los componentes físicos comprenden el *hardware*, el *software* y la infraestructura (los cables, los sistemas wireless, los enlaces electromagnéticos, los satelitales y los ópticos), que apoyan a las redes y a los conectores físicos (cables, radio frecuencia, *routers, switches, servers* y computadoras).

La capa lógica consiste en aquellos elementos de la red que se relacionan uno con el otro de manera que se abstraen de la red física, es decir, la forma o las relaciones no están vinculadas a un individuo, ruta de acceso específica o nodo. Un ejemplo simple es cualquier sitio web que está alojado en los servidores en múltiples ubicaciones físicas donde se puede acceder a todo el contenido a través de un localizador de Localizador Uniforme de Recursos (URL).

La capa de las ciber - persona consiste en la gente que se encuentra en un determinado momento presente en la red. Cabe destacar que un individuo puede tener múltiples

64 Traducción propia: Cyberspace Operations Concept Capability Plan 2016-2028, 20 Feb 2010 P. 8 Disponible en: http://www.acqnotes.com/Attachments/Cyberspace%20Operations%20Concept%20Capability%20Plan%202016-2028.pdf

65 Joint Publication JP 3-12 (R), Cyberspace Operations, Dated 5 February 2013. P. I-3.

ciber-persona, que pueden variar en el grado en que sean realmente exactas. Una sola ciber - persona puede tener varios usuarios. En consecuencia, la atribución de responsabilidad en el espacio cibernético es difícil.

Sin embargo, para el Reino Unido[66], el espacio cibernético debe considerarse compuesto de seis capas interdependientes: la social; la gente; la persona; la información; la red; y la real.

Comparando las definiciones anteriores, el espacio cibernético puede ser un espacio o un dominio; si es dominio, puede ser global y dinámico o solamente interactivo; puede ser un ambiente común, como los espacios terrestre, marítimo o espacial, o por el contrario ser transversal a los tres sin llegar a constituir un espacio en sí mismo (como lo señala la Directiva de Política de Defensa Nacional citada)[67]; abarca a las personas relacionadas con los sistemas informáticos durante el tiempo en que se encuentran interconectados conjuntamente con la tecnología de la información (informática) y la comunicación (telecomunicaciones) (TICs) conectada a Internet o solamente a esta última o aparte de ellas, también a las tarjetas chip, los sistemas de los automóviles, los electrodomésticos y los medios de transferencia de información.

Desde el punto de vista de la defensa, el espacio cibernético se utiliza cada día más, ya sea para recibir datos desde los centros de Comando y Control como para el desarrollo de las actividades de rutina, tales como capacitación, educación, médicas y logísticas y si bien la mayoría de los sistemas vitales tienen alternativas para superar el daño o la falla, la dependencia del espacio cibernético continúa en aumento. Pero también para el desarrollo de otras operaciones como las de información, las de apoyo de información militar [68](MISO), las de engaño y las de guerra electrónica.

De la misma forma, las amenazas actuales en el espacio cibernético son considerables; los ataques son continuos y permanentes, aunque totalmente diferentes de las operaciones militares convencionales en lo que respecta a métodos, alcances y consecuencias. Ello es así por diversas razones: en primer lugar, las defensas de los sistemas de las TIC y redes dependen de protocolos vulnerables y de arquitecturas abiertas, y la filosofía predominantemente defensiva enfatiza la detección de amenazas y no la eliminación de las vulnerabilidades.

En segundo lugar, los ataques en el espacio cibernético ocurren a gran velocidad, poniendo a las defensas bajo una gran presión, pues el atacante tiene que tener éxito una sola vez, mientras que el defensor tiene que ser exitoso todo el tiempo. En tercer lugar, la distancia ya no es un problema en el espacio cibernético ya que los ataques pueden ocurrir y ser ejecutados desde cualquier parte del mundo. En cuarto lugar, la atribución de los ataques es especialmente difícil, lo cual dificulta las posibles respuestas. Por último, la abrumadora dependencia de la sociedad moderna del espacio cibernético brinda a cualquier atacante un ambiente posible de ser atacado, lo que resulta en una gran presión sobre el defensor que debe defender con éxito el dominio.

---

66 Ministry of Defense, Development, Concepts and Doctrine Centre, Cyber Primer, (2nd Edition), 2016.

67 En el ámbito internacional, en el año 2016 EE.UU. y la OTAN lo han aceptado como un nuevo ámbito en sí mismo

68 Antiguamente denominadas Operaciones Psicológicas.

Cabe aclarar que, en el problema de la atribución, el hecho de asignar responsabilidad a un actor por un protagonismo o acción cibernética, la opinión de los técnicos está muy dividida: mientras algunos sostienen que en la determinación de la atribución es difícil tener certeza de autoría, otros sostienen que técnicamente es perfectamente posible determinar atribución. Probablemente en estas opiniones influya la política: aquellos países con fuerzas convencionales poderosas esgrimirán que, dado que la atribución es posible sin riesgo de equivocación, y que les cabe el derecho de tomar represalias con fuerzas convencionales en caso de ataques cibernéticos, esa opinión se sostenga por motivos disuasorios. Por otro lado, los poderosos del espacio cibernético y menos fuertes en fuerzas convencionales, sostendrán que no existe técnica posible de determinar atribución. Esta postura es un escudo protector gratuito.

Lo concreto es que para Casar Corredera[69] el espacio cibernético posee una serie de características diferenciales del resto de los espacios. En resumen:

- El espacio cibernético es un entorno único, en el que el atacante puede estar en cualquier parte del globo.
- En la defensa intervienen muchos factores, y no sólo elementos estatales sino también privados. Se exige pues una estrecha coordinación entre todos ellos.
- La confrontación en el espacio cibernético presenta frecuentemente las características de un conflicto asimétrico; y es frecuentemente anónimo y clandestino.
- Permite obtener información sobre objetivos sin necesidad de destruir ni neutralizar ningún sistema y, a menudo, sin delatarse.
- Permite también ejercer el chantaje; pero, al mismo, tiempo, la defensa puede utilizarlo para la disuasión.
- Evoluciona rápidamente siguiendo la evolución tecnológica de las TIC.

Por último, lo que debe tenerse presente es que[70]:

> El término ciberespacio no es neutral. Transmite varias representaciones algunas de las cuales, contradictorias entre sí, son el origen de varias concepciones del ciberespacio que se transcriben en las estrategias de los Estados. Estas representaciones se convierten en una herramienta de geopolítica. Algunos estados, como Rusia, han elegido en su estrategia no utilizar el término ciberespacio y prefieren el concepto de "espacio de información". El uso de un concepto más grande le permite a Rusia superar incluso el ciberespacio para permitir un control sobre la información de una manera global y sin tener en cuenta el vector por la cual se distribuye.

---

69 Casar Corredera, José Ramón, "El Espacio cibernético: Nuevo escenario de confrontación", Centro Superior de Estudios de la Defensa Nacional, Monografías del CESEDEN, febrero de 2012, P. 14; Disponible en: http://www.defensa.gob.es/ceseden/Galerias/destacados/publicaciones/monografias/ficheros/126_EL_ESPACIO CIBERNÉTICO_NUEVO_ESCENARIO_DE_CONFRONTACION.pdf

70 Desforges, Alix, Les représentations du cyberespace: un outil géopolitique; Disponible en: https://www.cairn.info/revue-herodote-2014-1-page-67.htm

> Sin ser un territorio aparte, los actores de los conflictos en el ciberespacio a menudo lo consideran como un mundo virtual (en oposición a uno real) generado por la interconexión de redes. Pero los conflictos geopolíticos en los que el ciberespacio es el objeto o el vector no son irreales, sino que son el reflejo de las rivalidades de poder existentes en otra parte. Ante todo, es una nueva forma de expresión de los conflictos.

Luego de haberse visto todas estas definiciones tan detalladas y densas, como señalan Singer y Friedman[71] "uno desearía volver a los tubos".

Guerra cibernética

Tal como lo expresó Luis Feliú[72] en una conferencia sobre Ciberdefensa,

> El conflicto armado es inherente a la historia de la humanidad. El ser humano ha tratado siempre de dirimir sus diferencias por medio de la violencia cuando las palabras, las razones y otras acciones han fracasado. Siempre es con la misma finalidad, la de infligirle un perjuicio de forma tal que se imponga la voluntad propia a la del adversario, quien se defenderá para tratar de impedir o minimizar este perjuicio y evitar el sometimiento de su voluntad, dando lugar a enfrentamientos. Históricamente, cuando son las colectividades las que se han enfrentado, dan lugar a los conflictos armados que se manifiestan por medio de combates o luchas y que tienen lugar, al principio, en espacios terrestres. Más tarde y al percatarse que desde el mar también es posible influir en la imposición de esta voluntad, surgen los combates navales y las acciones del mar sobre la costa, después aparecen de forma similar los combates en el aire y en el espacio. Cada vez que aparece una nueva dimensión real o virtual que el ser humano quiere utilizar, los contendientes tratarán de dominarla, de obtener la superioridad en ella, con objeto de poder actuar desde ella en su beneficio e impedir o dificultar su uso al adversario. Este ha sido el caso últimamente del espacio electromagnético y, más recientemente aún, del espacio cibernético o espacio cibernético. Estos conflictos armados entre estados han dado lugar históricamente a las guerras.

Para la Directiva de Política de Defensa Nacional 2645/14, "Las acciones de guerra cibernética poseen su origen en el ámbito virtual de las redes de comunicación y sistemas informáticos, sus efectos impactan sobre el mundo físico, pudiendo afectar, por ejemplo, el tráfico aéreo y terrestre, el control de las infraestructuras críticas, el abastecimiento energético y de agua potable, entre otros".

Ya en 1993, Arquilla y Ronfeldt[73] habían escrito un artículo *Cyberwar is coming* donde advertían que las futuras guerras girarían alrededor del conocimiento. Además, hi-

---

71 Singer y Friedman Op. Cit. P. 28

72 Feliú, Luis, Seguridad Nacional y Ciberdefensa, una aproximación conceptual, Conferencia en la UPM, Madrid 21 de enero de 2013; Disponible en: http://catedraisdefe.etsit.upm.es/wp-content/uploads/2013/01/Ponencia-Luis-Feliu.pdf .

73 Arquilla, John, Ronfeldt, David "In Athena's Camp Preparing for Conflict in the Information Age" Disponible en: http://www.rand.org/pubs/monograph_reports/MR880.html

cieron una distinción entre la "guerra cibernética" limitada a los sistemas militares y la "guerra de redes" más relacionada con el ámbito civil.

Sin embargo, de la misma manera que sucede con el término espacio cibernético, tampoco existe una definición universalmente aceptada respecto de lo que se entiende por guerra cibernética. Una definición general podría ser la de la Organización RAND[74], que define a la guerra cibernética como "la acción de un Estadonación para penetrar en las computadoras y las redes de otra nación con fines de causar daño o interrupciones a través, por ejemplo, de virus informáticos o ataques de denegación de servicio".

Para Blasco[75], "la guerra cibernética complementa la guerra tradicional y al mismo tiempo refleja sus usos y costumbres. También en la guerra cibernética hay soldados y espías: empleados de las fuerzas armadas y los servicios de inteligencia --muchos de ellos reclutados en universidades, pero también en el submundo de hackers delincuentes, dedicados a ejecutar misiones contra intereses de otros países".

Como en la guerra tradicional, en la guerra cibernética circulan mercenarios, lo que en inglés se llaman *hackers for hire,* (piratas de alquiler). De esta guerra también participan voluntarios, milicianos que creen en una causa: los llamados hackers patriotas. Blasco pone un ejemplo. "Si Ucrania entra en guerra con Rusia, hay hackers en Rusia que son patrióticos e intentarán hackear redes de defensa en Ucrania para dar esa información a su gobierno", dice. "No lo hacen por motivos financieros".

Para Conti y Surdu[76], "la guerra cibernética requiere no solo de habilidades técnicas, sino también de habilidades para solucionar problemas de creatividad, para actuar de manera equilibrada bajo presión y de pensamiento crítico. Los atributos que son deseables en los soldados, como la resistencia física, la puntería y las habilidades técnicas asociadas con el empleo de las fuerzas tradicionales y sistemas de armas, no se condicen con la guerra cibernética".

Es por ello que el adiestramiento de los que hoy en día se denominan "ciberguerreros" va mucho más allá de "adquirir habilidades". Algunos de ellos no solo poseen conocimientos sobre idiomas informáticos, sino que también se capacitan en idiomas extranjeros. Más aún, los Comandos de Ciberdefensa suelen incluir (o tener acceso regular a) personal con una buena comprensión de los matices culturales, la dinámica humana y las estrategias de influencia y persuasión. La guerra cibernética no siempre se trata de "ceros y unos; también puede implicar la intrusión de contenidos en las redes de los adversarios, un contenido distinto al código de la computadora que está diseñada para tener un impacto en el dominio cognitivo[77].

---

74 RAND Corporation, Cyberwarfare, Artículo febrero 2016; Disponible en: http://www.rand.org/topics/cyber-warfare.html.

75 Blasco, Jaime (director de los laboratorios de seguridad Alien Vault en Silicon Valley), El más fuerte es el más vulnerable, Diario El País, España, artículo del 7 febrero 2015; Disponible en: http://internacional.elpais.com/internacional/2015/02/07/actualidad/1423330690_981628.html .

76 Conti, Gregory, and John Surdu, "Army, Navy, Air Force, and Cyber—Is It Time for a Cyberwarfare Branch of Military?" IAnewsletter, Vol. 12, No. 1, Spring 2009, P. 17.

77 Christopher, Paul, Porche Isaac R. III, y Axelband Elliot; The Other Quiet Professionals Lessons for Future Cyber Forces from the Evolution of Special Forces; Disponible en: http://www.rand.org/pubs/research_reports/RR780.html

En abril de 2016, la Ministra de Defensa alemán Ursula von der Leyen detalló un plan para establecer, a partir del 1 de abril de 2017, un comando cibernético y de información que reunirá las unidades cyber e IT de las fuerzas armadas. El *Kommando Cyber-und Informationsraum* (Cyber y comando del espacio de información) será responsable de ciberinteligencia militar, geo-información y comunicación operacional.

Por último, según la Resolución 1113 (2011), adoptada por el Consejo de Seguridad de las Naciones Unidas el 5 de marzo de 2011, "guerra cibernética significa el uso de computadoras o medios digitales por un gobierno o con el conocimiento explícito o la aprobación de ese gobierno contra otro estado, o propiedad privada dentro de otro Estado incluyendo:

- El acceso intencional, interceptación de datos o daños a la infraestructura digital y a la infraestructura controlada digitalmente; y
- La producción y distribución de dispositivos que pueden usarse para subvertir la actividad interna.

La misma Resolución ONU observa la diferencia entre guerra cibernética interestatal e intraestatal, y actores no estatales que perpetran delitos cibernéticos; el aumento en el gasto de recursos en ciberofensiva nacional y en estrategias defensivas; destaca el hecho de que el delito cibernético cometido por actores no estatales requerirá de una defensa significativa en el futuro; y hace un llamamiento a todas las naciones para que cese el desarrollo y a repudiar el uso de tácticas de guerra cibernética. Es algo así como el pacto Briand – Kellogg[78] del siglo XXI.

Otra definición sería la que señala que: "la guerra cibernética es una actividad digital simétrica o asimétrica ofensiva y defensiva por parte de estados o actores que simulan ser estados, que resulta ser peligrosa para la infraestructura crítica nacional y los sistemas militares. Requiere un alto grado de interdependencia entre las redes digitales y la infraestructura por parte del defensor y de avances tecnológicos por parte del atacante. Puede entenderse como una amenaza futura en lugar de una presente y se ajusta perfectamente al paradigma de la Guerra de la Información[79]".

Para la República Federativa del Brasil[80], "guerra cibernética es el uso ofensivo y defensivo de la información y sistemas de información para denegar, explotar, corromper, degradar o destruir las capacidades de comando y control del adversario, en el marco de

---

78 El 27 de agosto de 1928 en París por iniciativa del ministro de Asuntos Exteriores de Francia, Aristide Briand, y del Secretario de Estado de los Estados Unidos Frank B. Kellogg, los quince estados signatarios se comprometían a no usar la guerra como mecanismo para la solución de las controversias internacionales. Hubo múltiples matices a este compromiso, por ejemplo, la guerra en defensa propia, las obligaciones militares que surgieran del pacto de la Liga de Naciones, la doctrina Monroe o los tratados de alianza acordados tras la I Guerra Mundial. Si se unen todas estas excepciones al hecho de que el tratado no estableció ningún método para forzar su cumplimiento, se puede entender como el Pacto resultó totalmente inútil.

79 Coughlan Shane M., "Is there a common understanding of what constitutes cyber warfare?" The University of Birmingham School of Politics and International Studies, 30 September 2003, P. 2.

80 Ministerio de Defensa de Brasil, Doutrina de Operações Conjuntas – MD30-M-01 / Volumes 1, P. 55/128, Año 2011; Disponible en: http://www.defesa.gov.br/arquivos/legislacao/emcfa/publicacoes/doutrina/md30_m_01_volume_1.pdf.

un planeamiento militar de nivel táctico/ operacional o de una operación militar. Estas acciones están diseñadas para obtener ventajas tanto en el área civil como en la militar".

De acuerdo a lo analizado hasta aquí se puede afirmar entonces que el término *guerra cibernética* es algo descriptivo que representa la lucha entre dos estados o facciones de los mismos que tiene lugar en el espacio cibernético.

Esto que hasta hace poco parecía ser un asunto de película de ficción ya ha dejado de serlo. La guerra cibernética o guerra "por control remoto" no es novedosa, pero es una estrategia que está irrumpiendo en los nuevos escenarios de conflicto, pues permite ser accionada a distancia. Incorpora nuevas tecnologías y las fuerzas que son necesarias desplegar dejan pocos rastros de su presencia. Ello habilita a quienes deben tomar decisiones de carácter estratégico a aprobar la ejecución de operaciones que difícilmente autorizarían si se emplearan en su lugar medios convencionales. Lanzar un ciberataque seguramente podría ser más barato y rentable que ejecutar un ataque físico.

Sin embargo, ciertos analistas discrepan sobre el uso de la palabra "guerra". A pesar de haberse tornado el principal tema por el que los estados e instituciones se refieren a ciberataques continuos, la palabra "guerra cibernética" no es unánimemente aceptada entre los especialistas en el tema, pues se trata de una cuestión semántica de aplicaciones prácticas.

El principal crítico de la expresión es Thomas Rid, profesor del Kings College de Londres, quien en su libro "*Cyber War Will Not Take Place*" argumenta que cualquier acto ofensivo, para ser considerado un acto de guerra, debe obedecer a tres criterios. En primer lugar, debe ser físicamente violento, es decir, debe haber víctimas. En segundo lugar, debe ser instrumental, o sea que la violencia debe ser un medio para alcanzar un fin. Por último, los actos de guerra son necesariamente políticos: un estado que busca dominar a otro.

Para Catherine A. Theohary y Anne I. Harrington[81] es difícil trazar líneas claras entre guerra cibernética, ciberdelito, ciberterrorismo y ciberespionaje. Diariamente los actores estatales y no estatales llevan a cabo "ataques cibernéticos". Cuándo y bajo qué condiciones esos ciberataques pueden considerarse como parte de una guerra cibernética entre estados nación es una cuestión pendiente de resolver.

Algunos expertos sostienen que toda guerra, e incluso la guerra cibernética, por definición incluye la destrucción de objetos físicos. Según este punto de vista, para ser considerado como un acto de guerra cibernética, el ataque debe originarse en el espacio cibernético y como resultado producir la destrucción de una infraestructura crítica, una capacidad de mando y control militar, o producir lesiones o la muerte de individuos.

En su artículo titulado *The Joint Force Commander´s Guide to Cyberspace Operations*[82] y a los efectos de determinar las tareas, propósitos y capacidades de los medios

---

81 Theohary, Catherine A. y Harrington, Anne I.; Cyber Operations in DOD Policy and Plans: Issues for Congress; January 5, 2015; Disponible en: https://www.hsdl.org/?view&did=761572

82 Williams, Brett T.; The Joint Force Commander´s Guide to Cyberspace Operations, Joint Forces Quarterly 73, National Defense University Press, April 2014; Disponible en: http://ndupress.ndu.edu/Media/News/News-Article-View/Article/577499/jfq-73-the-joint-force-commanders-guide-to-cyberspace-operations/

cibernéticos militares, Brett Williams define cuatro axiomas en el uso del espacio cibernético. El primero de ellos, se opone a la frase *guerra cibernética* y prefiere el de *operaciones militares cibernéticas*, puesto que la primera tiende a incrementar la relevancia de las operaciones cibernéticas por sobre otras actividades contribuyentes también a lograr los objetivos del Plan de Campaña.

En coincidencia con Williams, Herr Trey[83] señala que:

> ...operaciones militares cibernéticas (MCO por su denominación en inglés) es un término genérico para la adquisición y uso de capacidades cibernéticas en los niveles estratégicos, operacionales y tácticos del conflicto. MCO no es lo mismo que "guerra cibernética". La ciberguerra, como generalmente se llama, se centra en dos (o más) combatientes que exclusivamente despliegan capacidades cibernéticas maliciosas contra los sistemas de la otra parte, dando por resultado muerte y destrucción, para alcanzar un conjunto de objetivos políticos explícitos. Esta formulación, sin embargo, ignora la actual doctrina militar de Estados Unidos y la manera en que las fuerzas modernas realmente implementan tales capacidades. De hecho, son potencialmente buenas razones para creer que la ciberguerra, cuando se define correctamente, realmente no tiene lugar o puede constituir una herramienta de política ineficaz.

Otros analistas tienen una visión más inclusiva de la guerra cibernética. Estos expertos incluirían, además de los ataques cibernéticos con efectos cinéticos, la exfiltración[84] o corrupción de datos, la interrupción de los servicios, o la manipulación de las víctimas a través de la distracción[85].

En el extremo opuesto del debate están Peter Singer y Allan Friedman[86], autores de "*Cybersecurity and Cyberwar*" que admiten una interpretación más elástica del término "guerra" pues para ellos, definir si la guerra cibernética es o no una guerra no puede ser algo tan complicado.

> Todos los elementos clave de la guerra en el espacio cibernético tienen sus paralelismos y conexiones con la guerra en otros dominios. Ya sea en tierra, en el mar o en el aire, o ahora en el espacio cibernético, la guerra siempre tiene un objetivo político y un modo (que la distingue de la delincuencia) y siempre tiene un elemento de la violencia. Actualmente, la posición del gobierno de Estados Unidos es que, para cumplir con esta definición de uso de la fuerza, un ataque cibernético tendría que "resultar en una muerte, heridas o en una destrucción significativa" Es decir que, si incluso se realiza a través de medios cibernéticos, el efecto debe ser daños físicos o destrucción.

---

83 Herr, Trey and Herrick, Drew, Military Cyber Operations: A Primer, The American Foreign Policy Council Defense Technology Program Brief, January 2016, Washington DC, # 14; Disponible en: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2725275

84 Exfiltrar: neologismo por sacar a hurtadillas, antónimo de infiltrar.

85 Esta definición se ajusta a la actual vigente en ONU.

86 Singer P. W. & Friedman Allan; Cybersecurity and Cyberwar What Everyone Needs to Know; Op. Cit. P. 125.

Para proporcionar un paralelismo, un avión bombardeando está empeñado en una guerra aérea; un avión arrojando folletos, no tanto.

No obstante, para estos dos autores, "en una parte importante de estas discusiones, respecto de si es o no una guerra, a menudo se olvida que, aunque nos gustaría pensar que la ley es la guía de nuestro comportamiento, delinear claramente cuándo un ataque cibernético escala a una guerra no es sólo una cuestión de derecho internacional o sólo para que los abogados decidan". Como Carl von Clausewitz escribió, "la guerra no es un fenómeno independiente, sino la continuación de la política por medios diferentes." La guerra es política, y por ser política, es también siempre interactiva. Es decir, hay partes en la guerra, cada una con sus propias metas, acciones y respuestas, cada una tratando de doblegar la voluntad del otro.

Esta naturaleza fundamentalmente política de la guerra significa que todas estas preguntas respecto de cuándo un ciberataque alcanza a ser una guerra vendrá a través de decisiones políticas difíciles, en lo que Clausewitz vería como una versión digital de su famosa *"niebla de guerra"*, las circunstancias desordenadas, el movimiento rápido, y circunstancias poco claras que siempre acompañan a la guerra.

"En última instancia, guerra cibernética es lo que en el mundo real se cree que es. Al final del día, es el Presidente quien tiene que decidir si se trata de guerra u otra cosa. La norma es ambigua. Decidir cuándo algo es un acto de guerra no es automático, es siempre un tema de juicio[87]".

Agresión cibernética

A diario se conocen informes que señalan que tal gobierno, o grupo, o empresa, o ciudadanos han sufrido un "ataque cibernético". El pasado 5 de junio de 2015 el diario El País de España titulaba un artículo: "Un ciberataque afecta a millones de funcionarios de Estados Unidos." [88]

Quien hubiera ingresado en la página de *Cyberdefense Magazine*[89] del 24 de mayo de 2015 podría haber leído cualquiera de los siguientes artículos:

- El investigador en seguridad Patrick Barker descubrió que Samsung está deshabilitando *Windows Update* para ejecutar su propio *bloatware*[90] dejando a sus usuarios librados a ataques cibernéticos.
- El Instituto Nacional de Estandarización y Tecnología (NIST) comunica directivas de ciberseguridad para contratistas del gobierno.
- *Hackers* atacan a la aerolínea polaca LOT, dejando en tierra a 1400 pasajeros.
- El ciberdelito está pagando 1,425 por ciento de retorno a la inversión.

---

87 Singer P. W. & Friedman Allan; Cybersecurity and Cyberwar What Everyone Needs to Know; Op. Cit.

88 Diario El País, Sección Internacional, artículo Un ciberataque afecta a millones de funcionarios en EEUU, 5 Junio 2015; Disponible en: http://internacional.elpais.com/internacional/2015/06/05/actualidad/1433458231_191963.html

89 Cyberdefense Magazine, edición del 24 de mayo de 2015; Disponible en: http://www.cyberdefensemagazine.com/newsletters/may-2015/index.html .

90 Software bloat: es el resultado de la adición de nuevas características a un programa o sistema en el punto donde el beneficio de las nuevas características es preponderante por sobre los recursos extras consumidos (RAM, espacio en disco o rendimiento) y la complejidad de uso.

- La computadora personal de la canciller alemana Ángela Merkel fue la primera infectada en el hackeo al *Bundestag*.
- Un investigador encuentra que las turbinas eólicas y los sistemas solares son vulnerables mundialmente.
- Los datos de la Oficina de Personal de los Estados Unidos (OPM) se ofrecen a la venta en la "Web negra".
- Un experto en seguridad demostró cómo explotar la vulnerabilidad del sistema Apple IOS para robar la contraseña de un usuario por medio de un *phishing mail*.
- Las autoridades de Bélgica detienen a terroristas interceptando mensajes de *WhatsApp*.
- Los hackers del Ejército Electrónico Sirio borraron la página Web del Ejército de los Estados Unidos accediendo a través de *Limelight Networks* que es una compañía de entrega de contenidos digitales.
- La Fuerza Aérea de los Estados Unidos localizó un comando del ISIS[91] analizando una *selfie*.
- Los *hackers* chinos tuvieron acceso a millones de registros de trabajadores estadounidenses.

Quien ese mismo día hubiese leído la segunda página del matutino "La Nación" se hubiera encontrado con un artículo titulado: "En la terraza, un sistema sofisticado de escuchas; Tensión entre aliados / Otro escándalo para la Casa Blanca[92]" En el artículo se señala que:

> ... para interceptar las comunicaciones del Palacio del Elíseo y de los principales ministerios franceses, la Agencia Nacional de Seguridad (NSA) utiliza un sofisticado sistema electrónico instalado en la terraza de la embajada de Estados Unidos de París. El dispositivo, que fue montado entre 2004 y 2006, está oculto por una carpa rectangular del mismo color que el edificio diplomático y que tiene falsas ventanas pintadas. El material de esa tienda de campaña permite ocultar las antenas y no perturba el paso de las ondas electrónicas para poder escuchar clandestinamente las comunicaciones telefónicas del palacio presidencial, la Asamblea Nacional, la cancillería y los ministerios de Interior, Justicia y Defensa, ubicados en un radio de 800 metros.
>
> El sistema es similar al que funciona en el último piso de la embajada de Estados Unidos en Berlín, a pocos pasos de la cancillería alemana y que fue denunciado cuando se reveló que la National Security Agency monitoreaba el modesto celular Nokia de primera generación que utilizaba Ángela Merkel. Otras instalaciones de la misma

91 ISIS: Islamic State in Iraq and Syria; anterior nombre de la organización Estado Islámico.

92 Cabe destacar que la diferencia entre ciberespionaje y ciberdelito generalmente determina los órganos del Estado que tienen la responsabilidad de actuar frente a dichos actos y de enjuiciar a quienes los cometen. Las fuerzas de seguridad y policiales suelen tener la responsabilidad de disuadir y perseguir los delitos cibernéticos. Las organizaciones de contrainteligencia, que pueden ser parte de las comunidades policiales, militares o de inteligencia del Estado generalmente manejan los casos de ciberespionaje.

naturaleza existen en Ginebra, Madrid, Viena, Roma, Estocolmo, Varsovia y otras 13 capitales de primera importancia estratégica en Europa".

Un combatiente de la oposición siria conectado a su ordenador, una mujer libanesa llamada Imán que aparece en pantalla. Una breve conversación vía chat a través de la red de mensajería instantánea Skype, un intercambio de fotos. Imán envía una fotografía "personal" al soldado. Éste la abre. Ya está: el Dark Comet RTA (siglas de Troyanos de Acceso Remoto) que esconde la imagen, virus capaz de secuestrar información del ordenador, acaba de penetrar una computadora de las fuerzas que combaten al régimen de Bachar El Assad[93].

De hecho, organizaciones como Al-Qaeda o ISIS, emplean Internet con el fin de difundir información verdadera o falsa, adiestrar a sus agentes, o captar seguidores.

Cabe entonces preguntarse, ¿cuál es la validez del concepto de agresión expresado en la Resolución ONU 3314/74 titulada *Definición de la agresión*? ¿Cuál o cuáles de toda esta muestra de incidentes cibernéticos pueden ser considerados por los analistas vernáculos como "agresiones militares estatales externas" que afectan según esta particular forma de razonar, específicamente el ámbito de la Defensa Nacional?

¿Puede ser considerado como un ataque el acceder a una computadora (o sistema de cómputos) sin autorización, o excediendo el nivel de acceso autorizado y, por medio de esa conducta, obtener información? Pareciera ser que lo que el diario "El País" de España titula como un ataque, en realidad sería lo que una fuerza de seguridad caratularía como una "intrusión cibernética" y, por tanto, constituiría un delito y no un ataque cibernético que pudiera dar lugar a llevar a cabo una acción militar, incluso la guerra.

Sin embargo, para Catherine A. Theohary y John Rollins[94] los objetivos de un ataque cibernético pueden incluir las siguientes cuatro áreas:

- pérdida de la integridad, de manera tal que la información pudiera llegar a ser modificada inadecuadamente;
- pérdida de disponibilidad, donde los usuarios autorizados no pueden acceder a los sistemas críticos para el cumplimiento de la misión;
- pérdida de confidencialidad, donde se revela información crítica a usuarios no autorizados; y
- destrucción física, donde los sistemas de información crean un daño físico real, a través de comandos, que causan malfuncionamientos deliberados.

Asumiendo que se dispone de la capacidad para atribuirle a un Estado el ataque a un

93 Elola, Joseba; "Así es un ataque, paso a paso". Diario El País, España, 7 febrero 2015; Disponible en: http://internacional.elpais.com/internacional/2015/02/06/actualidad/1423238838_807110.html .

94 Congressional Research Service, Theohary Catherine A. y Rollins John "Terrorist Use of the Internet: Information Operations in Cyberspace" March 8, 2011 Disponible en: https://www.fas.org/sgp/crs/terror/R41674.pdf.

objetivo del sistema de defensa propio, cabe preguntarse si dicho ataque constituye un "ataque armado" o una "agresión militar estatal externa" en el espacio cibernético. Si se trata de un ataque porque se ha tomado la iniciativa, habría que discutir si se trata de un ataque con armas y si las redes de computadoras o los dispositivos USB pueden considerarse un arma. Si se trata de agresión, habría que considerar si se trata de una agresión externa a las fronteras o fue generada en el mismo país, si fue estatal, de agentes del estado, de hackers contratados por el estado, de hackers individuales patrióticos, o de estudiantes del secundario ociosos. En cuanto a determinar si es militar, habría que analizar si fue contratada por militares, si los que la ejecutaron tenían o no uniforme, o fue por iniciativa privada. Como puede verse, las variables son muchas.

El derecho internacional vigente establece, en primer lugar, las circunstancias bajo las cuales un estado puede ir a una guerra contra otro - *jus ad bellum* - y, en segundo lugar, cómo los militares deben conducirse una vez que están en guerra, con el fin de minimizar el sufrimiento humano – *jus in bello*. Bajo la carta de las Naciones Unidas, un estado tiene el derecho de utilizar la fuerza contra otro estado para defenderse de un "ataque armado", per se o si está autorizado por el Consejo de Seguridad. La conducta de los militares una vez en guerra se rige por los convenios de Ginebra y La Haya.

Entre los principios fundamentales de los Convenios de Ginebra se encuentra aquel que establece que el daño infligido en un ataque militar debe ser "proporcional" al objetivo y que se deben evitar objetivos civiles ejerciendo la "discriminación" entre combatientes y no combatientes. La aplicación de esos principios a la guerra cibernética es problemática. Un oficial puede utilizar algoritmos para predecir el daño que ha de causar una bomba, en función de su tamaño, del ángulo de aproximación y de la fuerza del blanco, pero un ataque a una red informática puede tener efectos impredecibles. La dispersión geográfica de las infecciones del gusano informático *Stuxnet* sugiere que un arma cibernética, a pesar de su extraordinaria precisión, no puede ser controlada fácilmente una vez que ha sido liberada[95]. Hasta ha pasado en actos de represalia entre compañías informáticas, en los que una represalia DDOS de una de ellas sobre la otra motivó como "daño colateral" la caída de las redes de Internet en toda Europa.

Para el experto Gary McGraw[96] el ataque a Irán constituyó un ciberataque por cuanto *Stuxnet* hizo lo que pudo en Irán para arruinar los sistemas físicos de control de centrifugadoras o que en realidad eran nuevas centrifugadoras en sí mismas que reemplazaron los algoritmos de las primeras. El presidente iraní Mahmoud Ahmadinejad admitió que hubo un ataque cibernético en las centrifugadoras. Aunque ningún estado reclamó autoría, es fácil deducir que quien preparó al *Stuxnet* debía conocer el funcionamiento de las centrifugadoras, las características de las plantas y los sistemas de control. Está claro que solo un estado puede tener acceso a tantas fuentes de información.

---

95 Gjelten, Tom. Shadow Wars: Debating Cyber 'Disarmament World Affairs; November/December 2010; Disponible en: http://www.worldaffairsjournal.org/article/shadow-wars-debating-cyber-disarmament.

96 Dunlap, Charles J. Jr, "Perspectives for Cyber Strategists on Law for Cyberwar" Strategic Studies Quarterly; Spring 2011; P 86; Disponible en: http://cyber.law.harvard.edu/cybersecurity/Perspectives_for_Cyber_Strategists_on_Law_for_Cyberwar

Por otro lado, para McGraw el ataque a Estonia no lo fue, por cuanto, por un lado, no fue perpetrado por un Estado- nación y por otro, un ciberataque necesita tener un impacto cinético, es decir, debe lograr que algo físico deje de funcionar o funcione incorrectamente.

En línea con este concepto, el Mayor General Dunlap[97], partiendo de lo que escribe Michael N. Schmitt en su trabajo "*Cyber Operations in International Law*" respecto de que la "esencia de una operación 'armada' es la relación de causalidad o riesgo, de muerte o lesiones a personas o daños a, o destrucción de bienes y objetos tangibles", deduce que "los eventos cibernéticos que tienen efectos violentos suelen ser, por lo tanto, el equivalente legal a los ataques armados".

Para ser más claro, expresa que no todos los eventos cibernéticos califican como ataques; por consiguiente, antes de responder de una manera que constituya un uso de la fuerza – lo cual incluye acciones que incluso no equivalen a un ataque armado - las evidencias tienen que mostrar que la cantidad de efectos desencadenantes, son equivalentes a un ataque armado. Si no llegasen a alcanzar tal nivel, la respuesta debe limitarse a actos que equivalgan a un uso de la fuerza. Evaluar desapasionadamente las consecuencias de un incidente cibernético para determinar su similitud con un ataque armado puede ser difícil, como también pueden ser ampliamente magnificadas las primeras impresiones de los efectos causados por él.

En cualquier caso, las operaciones cibernéticas ofensivas deben utilizarse de manera discriminada, teniendo siempre presente que los ataques militares solo están dirigidos contra objetivos militares. Únicamente un objetivo militar es un legítimo objeto de ataque directo, entendiéndose como tal, "aquel objeto cuya destrucción total o parcial, captura o neutralización ofrece una ventaja militar directa y concreta". La discriminación es bastante amplia en su interpretación, porque si la población civil se ve afectada, eso afecta la moral del pueblo que combate. Era el razonamiento de Winston Churchill cuando se le cuestionó el bombardeo de Hamburgo y Dresde, que eran ciudades sin soldados con mujeres, chicos y heridos de guerra. Churchill contestó que "la moral del enemigo es un objetivo militar".

De lo hasta aquí expresado, puede deducirse que para que un ciberataque pueda ser considerado como un "ataque armado" por el Derecho Internacional de los Conflictos Armados, este debería lograr que algo físico deje de funcionar o funcione incorrectamente. Claro está que la interpretación final recaerá en el que tiene mayor poder en armas convencionales.

Restaría analizar si, tal como lo señala la Directiva de Política de Defensa Nacional argentina de marras, al limitar la respuesta de las Fuerzas Armadas a una agresión militar estatal externa, es posible en la actualidad determinar por parte de un estado- nación que ha recibido un ataque, si este fue perpetrado por otro estado, o si ese otro estado conocía o había aprobado que un grupo no militar de ese estado emplease computadoras o medios digitales para actuar contra dicho país.

---

97 Dunlap, Charles J. Jr, "Perspectives for Cyber Strategists on Law for Cyberwar" Strategic Studies Quarterly; Spring 2011; P 86; Disponible en: http://cyber.law.harvard.edu/cybersecurity/Perspectives_for_Cyber_Strategists_on_Law_for_Cyberwar

Para la mayoría de los expertos, las sospechas de ciberataques patrocinados por un estado aun cuando a menudo pueden ser contundentes, son difíciles de probar. El relativo anonimato en el que operan los actores en el espacio cibernético brinda un grado de plausible negación.

Lo cierto es que cualquier sistema de defensa nacional necesita identificar al potencial adversario y anticiparse a las consecuencias de un ataque, cosa que para algunos sería difícil de ejecutar en el espacio cibernético, pues para poder estar en condiciones de imputar un ataque a otro estado, o a alguien apoyado por él, el o los estados afectados debieran disponer de todos los medios necesarios para establecer la "atribución", es decir, para hacer forensia[98] informática y ver si el ataque proviene de donde realmente se considera.

Para el Profesor Uzal, "La atribución de Ciberagresiones a un responsable específico constituye un asunto no trivial. La complejidad de la solución del Problema de la Atribución ha sido utilizada, por determinados gobiernos, como sustento de importantes campañas comunicacionales destinadas a difundir el mito de la imposibilidad de solucionar el mencionado problema"[99].

Igual que si se tratase de un ataque físico, en la actualidad se han ido creando impedimentos (antivirus y firewall[100]) para impedir ingresos no deseados, hackers, malware, virus, etc. Sin embargo, ello pareciera no ser suficiente para encontrar a los atacantes aun cuando para Uzal, que es uno de los que sostiene que identificar la atribución es posible, "los flujos de red correspondientes a Ciberagresiones pueden ser detectados, mediante el estudio del comportamiento estadístico de los routers, sin violar derechos humanos básicos tales como confidencialidad o la intimidad."[101]

Además, y más allá de los fundamentos técnicos, la atribución suele ser vista de manera distinta en cada nivel de la guerra.

Para Thomas Rid y Ben Buchanana[102], del *Department of War Studies del King's College of London*, en el nivel táctico, la atribución es tanto un arte como una ciencia.

---

98 Forensia: eufemismo por llevar a cabo pericias legales.

99 Uzal, R, et al, Lavado Transnacional de Activos en el Espacio cibernético. Presentación del contexto, planteo del problema y formulación de propuestas, Anales 44JAIIO, 2015 P. 56 Disponible en: http://44jaiio.sadio.org.ar/sites/default/files/Programa%2044%20JAIIO.pdf.

100 Firewall (cortafuegos): es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas. Se trata de un dispositivo o conjunto de dispositivos configurados para permitir, limitar, cifrar, descifrar, el tráfico entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios.

101 Un informe técnico de la compañía FireEye Inc. con sede en California, analizó una parte avanzada de malware, llamado HAMMERTOSS y conectó la herramienta a una banda de ciberespionaje conocida como APT29. Aunque no podría encontrar ningún vínculo directo con el Kremlin, FireEye dijo que la inteligencia solicitada por APT29 era más consistente con los intereses del gobierno ruso que con los de una típica empresa criminal. "Durante mucho tiempo, este grupo ha estado robando información que no puede ser monetizada. Van tras estos datos debido a su valor de inteligencia".
Durante el seguimiento de las actividades de APT29, los investigadores de FireEye encontraron muchos datos que indicaban que el grupo de hacking era estatal y no criminal. Por ejemplo, las actividades del grupo coincidían con las horas de trabajo del huso horario +3, que comprende a ciudades como Moscú y San Petersburgo, y los hackers parecían dejar de trabajar en días festivos rusos. "Si estos son delincuentes, son criminales comportándose de la forma en que lo haría un gobierno" FP Foreign Policy July/Aug 2015 Edition http://foreignpolicy.com/2015/07/29/does-the-kremlin-have-a-new-way-of-hacking-the-west-hammertossfireeye-apt29/ Se requiere suscripción a la revista.

102 Rid, Thomas & Buchanana Ben; Attributing Cyber Attacks Journal of Strategic Studies; 23 Dec 2014 Disponible en: http://dx.doi.org/10.1080/01402390.2014.977382

No existe una receta para realizar una atribución correcta, ni una metodología o un organigrama o una lista de verificación. Encontrar las pistas correctas requiere de un enfoque disciplinado dentro de un conjunto de preguntas detalladas, pero también de la intuición de operadores experimentados. Se requiere de un correcto *coup d'oeil*[103], para usar un término militar.

En el nivel operacional, la atribución es un proceso lleno de matices, y no es un problema simple. El proceso de atribución no es binario, sino que se mide en grados desiguales, no es blanco y negro, sí o no, por el contrario, aparecen distintos tonos. Es un trabajo de equipo, pues el éxito de la atribución requiere más habilidades y recursos que ninguna mente individual puede ofrecer. La optimización de los resultados requiere de un manejo cuidadoso y de un proceso organizativo. Además, y como en cualquier otra guerra, la percepción ocupará un lugar importante. No sería la primera guerra desatada por una percepción errónea.

Finalmente, en el nivel estratégico, la atribución es una función de lo que está en juego políticamente. Los riesgos políticos son determinados por una serie de factores, entre los cuales, lo más importantes, son los daños ocasionados. Dichos daños pueden llegar a ser una ofensa a la reputación de un país o un perjuicio físico o financiero. Visto desde arriba, la atribución orienta los procesos internos; participa en las evaluaciones finales y en las decisiones; y comunica los resultados a terceros y al público.

Por ello, en cuanto a la atribución de un ataque sobre las fuerzas propias, para evitar efectos contrapuestos, el nivel operacional debería centrar sus esfuerzos en determinar la arquitectura del nivel del ataque y el perfil del agresor - el qué, dejando para el nivel estratégico la comprensión de quién es responsable por el ataque, evaluar su justificación, su significación y dar la respuesta adecuada; y para el nivel táctico la comprensión de los hechos sobre todo en sus aspectos técnicos, o sea, el cómo.

Es por todo ello y porque aparentemente resultaría más fácil realizar un ataque que establecer un buen sistema de ciberdefensa, que se acuñó el término ciberdisuasión. Dado que no es objeto de esta obra hurgar sobre cada expresión que aparece, simplemente se dirá que cualquier tipo de disuasión tiene esencialmente tres componentes básicos: primero, la expresa intención de defender un determinado interés; en segundo lugar, la posibilidad de comunicar fehacientemente tal intención y por último, la capacidad demostrada para realmente lograr la defensa de los intereses en cuestión, o de infligir un costo sobre el atacante que, incluso si él es capaz de obtener su objetivo, la relación costo – beneficio le será totalmente desfavorable. Ya existen opiniones que tal cual se ha hecho con las armas nucleares, los mismos tipos de acuerdo deberían alcanzarse en armas cibernéticas. Existen hasta intentos de firmar acuerdos de no proliferación cibernética al igual que se hace con las armas nucleares en los tratados SALT (*Strategic Arms Limitation Treaty*) que comenzaron en el año 1972 entre Estados Unidos y Rusia, y permanecen hasta el último acuerdo de 2010.

---

103 von Clausewitz Carl, On War, traducido por Michael Howard and Peter Paret (Princeton University Press 1976), P. 100–12. Carl von Clausewitz utiliza coup d'oeil (golpe de vista) para describir al "genio militar" el "ojo interno" que permite a los buenos comandantes tomar las correctas decisiones bajo presión, sobrecarga de información y limitaciones de tiempo.

En concreto, en lo que respecta a la agresión cibernética podría decirse que ella sería considerada un ataque armado solamente cuando su finalidad haya sido la de negar, degradar, interrumpir y/o destruir un objetivo.

Tampoco debe olvidarse que existen diferentes niveles de guerra. El objetivo táctico de la atribución es la comprensión de los hechos sobre todo en sus aspectos técnicos, el cómo. El objetivo operacional es la comprensión de la arquitectura del nivel de ataque y el perfil del agresor — el qué. Por su parte, el objetivo estratégico es la comprensión de quién es responsable por el ataque, evaluar la justificación del ataque, su significación y dar la respuesta adecuada, el quién y por qué. Finalmente, la comunicación es también una meta en sí misma: comunicar los resultados de una investigación forense que emplea mano de obra intensiva es parte integrante del proceso de atribución y no debe ser tratado con baja prioridad. El dar a conocer públicamente una atribución puede tener efectos significativos: los atacantes pueden cancelar una operación, cambiar de táctica o reaccionar públicamente a las acusaciones y así se forma la respuesta más amplia del atacado.

Operaciones cibernéticas

El Decreto 2645/2014 (Directiva de Política de Defensa Nacional) también señala que:

> Dentro de la amplia gama de operaciones cibernéticas, sólo una porción de estas afecta específicamente el ámbito de la Defensa Nacional. En efecto, en materia de ciberdefensa existen dificultades fácticas manifiestas para determinar *a priori y ab initio* si la afectación se trata de una agresión militar estatal externa. Por tal motivo, resulta necesario establecer dicha calificación a posteriori actuando como respuesta inmediata el Sistema de Defensa, únicamente en aquellos casos que se persiguieron objetivos bajo protección de dicho sistema, es decir que poseen la intención de alterar e impedir el funcionamiento de sus capacidades.

Para entender las operaciones cibernéticas, quizás resulte necesario analizar las operaciones de inteligencia.

Indagando en la historia, se puede apreciar que las actividades de inteligencia fueron incrementando su valor en la medida en que mejoraban los medios para obtener información que los oponentes trataban de mantener en secreto. Fue así que al principio se dependió de los espías y luego de la capacidad para descifrar códigos. Luego sobrevino la capacidad de obtener fotografías desde el aire y más tarde desde el espacio.

En la medida en que mayor cantidad de información comenzó a ser digitalizada y las comunicaciones pasaron a ser instantáneas, los desafíos pasaron a ser mayores en virtud de la gran cantidad de material al que se puede acceder tanto de manera lícita o abierta, como ilícitamente o encubierta.

Luego pasó a ser otro desafío el de mantener la integridad de dicha información, a pesar de los intentos de interrumpirla o de atacarla a través de formas digitales de penetración conocidos como virus, troyanos, gusanos informáticos que afectan a equipos con Windows, llevadas a cabo desde servidores distantes.

Si bien muchas de estas actividades ilícitas tenían y tienen propósitos criminales y fraudulentos, existen ejemplos de robo de información gubernamental y de secretos de empresas y corporaciones llevados a cabo por hackers financiados por gobiernos, ataques que dañaron sistemas críticos, y virus misteriosos que dañaron programas nucleares (*Stuxnet*). No obstante, debe quedar claro que las operaciones cibernéticas no solo buscan secretos industriales ni llevan a cabo operaciones de espionaje, sino que llevan a cabo operaciones de información para hacer equivocar al enemigo en sus decisiones, y operaciones de redes y sistemas de redes para alterar el funcionamiento de los sistemas cibernéticos en los que los algoritmos reemplazan a la decisión del hombre.

La amenaza fue ganando credibilidad en la medida en que con cada vez mayor frecuencia distintas redes tanto civiles como militares eran atacadas por hackers, algunas veces independientes y otras veces motivados por los estados. Fue así que la protección de esas redes pasó a ser un tema de alta prioridad. Estos ataques y esta protección se llevan a cabo mediante lo que se ha dado en conocer como operaciones cibernéticas o ciberoperaciones.

Hasta este momento, las operaciones cibernéticas son consideradas como operaciones complementarias a las tradicionales, y por lo tanto tenidas en cuenta después que se formula el Plan General de Maniobra. Sin embargo, en el caso de la guerra entre Georgia y Rusia y entre Rusia y Ucrania, pareciera ser que ha ocurrido lo contrario, y se ha tomado a las operaciones cibernéticas como operación principal. Se dice – es difícil corroborar esta información porque ambos bandos lo ocultan – que el Ministro de Defensa de Ucrania debió emigrar a otro país para poder dirigirse a sus fuerzas, ya que su acceso a los medios de comunicación ucranianos le estaba técnicamente vedado.

Para España[104], las ciberoperaciones son el empleo de capacidades cibernéticas cuyo propósito es la consecución de objetivos militares en el espacio cibernético o a través de este. Las ciberoperaciones no son un fin en sí mismas, sino que forman parte integral de cualquier tipo de operación militar y su concepto surge de manera inmediata al considerar el espacio cibernético una dimensión más de las operaciones en un Teatro de Operaciones.

Para ser más claros, se puede ver lo que el Teniente Coronel del Ejército del Aire Javier López de Turiso explica en un escrito[105]:

> Se precisan sistemas de armas para hacer sentir el poder terrestre, naval o aéreo. En el espacio cibernético no, las armas no son cinéticas. Aquí también existen armas defensivas y ofensivas, pero son de índole totalmente diferente" y añade que "en el espacio cibernético el principal valor es la información, la que en la acción defensiva se ha de proteger y en la ofensiva se ha de negar, alterar o sustraer al enemigo". Y conclu-

104 Ministerio de Defensa de España, Centro Superior de Estudios de la Defensa Nacional (CESEDEN); Documentos de Seguridad y Defensa 44 "Adaptación de la Fuerza Conjunta a la Guerra Asimétrica"; septiembre de 2011, P. 47; Disponible en: http://www.defensa.gob.es/ceseden/Galerias/destacados/publicaciones/docSegyDef/ficheros/DSEGD_44.pdf.

105 Citado por Fernando Rueda, Artículo Preparados para la guerra cibernética; Diario El Tiempo de España, 12 febrero 2013; Disponible en: http://www.tiempodehoy.com/espana/preparadospara-la-guerra cibernética

ye: "Así como los conflictos tradicionales se centran en el campo de batalla, el espacio cibernético extiende la zona de combate hasta el mismo corazón de la nación, al ser capaz de entrar en cada una de las casas de los ciudadanos y de cortarle los suministros básicos que este necesita para su supervivencia".

Tal como sostiene Gómez Arriaga,[106]

> Las ciberoperaciones deberían entenderse como un instrumento más para la solución de problemas militares en su amplio espectro y, por lo mismo, implican eventualmente enfrentar a un antagonista. Pueden, por tanto, ser defensivas cuando buscan detectar, neutralizar y mitigar el impacto de un ataque; o bien, ser ofensivas cuando se utilizan para obtener inteligencia a través del espacio cibernético o para negar su empleo. Es decir, las ciberoperaciones implican intencionalidad, voluntades contrapuestas y el enfrentamiento en el espacio cibernético con fines militares, elementos clave que permiten distinguir las ciberoperaciones de otras actividades como la seguridad informática o las operaciones de información.

Para Francia[107], las operaciones en el espacio cibernético incluyen acciones defensivas (lucha informática defensiva LID), las acciones de exploración (u exploración informática, IE) y las acciones ofensivas (o lucha informática ofensiva, LIO). Todas ellas son conducidas por la cadena de comando operacional de defensa cibernética.

Para el Reino Unido[108], las operaciones cibernéticas son la planificación y sincronización de actividades en y a través del espacio cibernético para permitir la libertad de maniobra y, de esa manera, alcanzar los objetivos militares. Pueden categorizarse en cuatro funciones distintas: las operaciones cibernéticas defensivas (DCO); las operaciones cibernéticas ofensivas (OCO); las operaciones de ciber inteligencia, vigilancia y reconocimiento (IVR); y las operaciones cibernéticas de preparación operacional del ambiente.

Las DCO son medidas activas y pasivas tomadas para preservar la habilidad de usar el espacio cibernético. La defensa activa son actividades que atacan las operaciones ofensivas hostiles, a fin de preservar la libertad de maniobra en el espacio cibernético y la defensa pasiva son las medidas específicas tomadas para reducir la eficacia de la actividad cibernética.

Las operaciones cibernéticas ofensivas (OCO) son actividades que proyectan el poder para lograr objetivos militares en o a través del espacio cibernético. La actividad ofensiva cibernética puede utilizarse para infligir efectos temporales o permanentes y, así, reducir la confianza de un adversario en redes o capacidades. Dicha acción puede

---

106 Gómez Arriagada, Héctor; "Ciberoperaciones"; Revista Marina Chile 4 /2013; P. 46; Disponible en: http://revistamarina.cl/revistas/2015/2/hgomeza.pdf.

107 Centre interarmées de concepts, de doctrines et d'expérimentations, Les systèmes d'information et de communication (SIC) en opérations, Doctrine interarmées DIA-6_SIC-OPS (2014) N° 147/DEF/CICDE/NP du 24 juin 2014 Amendée le 16 janvier 2016, P. 71 t 72; Disponible en: http://www.cicde.defense.gouv.fr/IMG/pdf/20160116_np_dia-6_sic-ops_2014__amendee_janvier_2016.pdf.

108 Ministry of Defense, Development, Concepts and Doctrine Centre, Cyber Primer, (2nd Edition), 2016.

apoyar a la disuasión y comunicar intenciones o amenazas. En el nivel operacional/ táctico será necesaria una coordinación entre las operaciones cibernéticas ofensivas y las operaciones/ actividades de información.

Las operaciones cibernéticas ofensivas pueden categorizarse en siete etapas conocidas como "la cadena de un *ciberataque*"[109]:

1. **Comprensión:** adquirir la información e inteligencia en el ciberambiente de un blanco del adversario e identificar los objetivos específicos.
2. **Desarrollo de la capacidad de carga:** desarrollar los códigos de computadora (por ejemplo, *malware*) que crearán el efecto deseado explotando las vulnerabilidades identificadas del sistema a atacar.
3. **Entrega:** trasmitir la carga al sistema de destino usando vectores como: adjuntos de correos electrónicos, sitios web y medios extraíbles (por ejemplo, USBs).
4. **Explotación:** después de que la carga haya sido entregada al sistema de destino, la explotación desencadena la carga – explotando una aplicación o una vulnerabilidad del sistema operativo.
5. **Instalación:** instalar un acceso remoto o puerta trasera en el sistema de destino que permita al adversario mantener una presencia/persistencia dentro del sistema de destino.
6. **Mando y control:** el adversario establece canales de comunicación para facilitar la transmisión de comandos.
7. **Efectos deseados creados:** después de progresar a través de las seis primeras fases, el adversario puede tomar acciones para crear los efectos deseados por el atacante.

Las operaciones de ciberinteligencia, vigilancia y reconocimiento (cyber IVR) comprenden actividades en el espacio cibernético para reunir inteligencia activa de los sistemas del blanco y del adversario requeridos para apoyar las operaciones militares. Las misiones cibernéticas ISR para la defensa pueden ser apoyadas por las capacidades nacionales y/o de cada una de las fuerzas armadas.

Por su parte, las *operaciones cibernéticas de preparación operacional del ambiente* (cyber OPE) son todas las actividades que realizan par a preparar y posibilitar la ciberinteligencia, vigilancia y reconocimiento, y las operaciones defensivas y ofensivas. Estas son las operaciones típicas del nivel operacional de guerra.

Para el Reino Unido en el nivel estratégico, las operaciones defensivas aseguran la libertad de acción protegiendo la infraestructura y las capacidades desplegadas de la actividad ciberofensiva del adversario. En los niveles operacionales y tácticos, protegen los sistemas y las redes críticas que se encuentran en el mar, tierra, aire y espacio. Tal control suele localizarse en términos de tiempo y espacio y dependerá de la calidad de la información.

---

109 Ibidem.

La "*Doutrina Militar de Defesa Cibernética*"[110] de Brasil, al igual que la de España y Francia clasifican a las operaciones cibernéticas solamente en ofensivas, de protección y de exploración.

Según la doctrina brasilera, las ofensivas comprenden las acciones para interrumpir, negar, degradar, corromper o destruir informaciones o sistemas de computación almacenados en dispositivos o redes de computadoras o de comunicaciones del oponente. Las de protección son aquellas que se llevan a cabo de manera permanente con la finalidad de neutralizar los ataques o la exploración cibernética contra las computadoras o redes de computadoras y de comunicaciones propias e incrementan las acciones de seguridad y defensa en una situación de crisis o conflicto.

Para López[111], los objetivos de las operaciones ofensivas podrán ser:

- Propagación de virus computacionales para contaminar el flujo de la información enemiga.
- Controlar los elementos temporales (Internet) mediante la conducción de iniciativas en el ámbito de la información tendientes a inducir, engañar, encubrir, o contener.
- Interrumpir o sabotear la información o el sistema de información del enemigo (por ejemplo, bombardeando sus sistemas de comunicaciones), así como su estructura para la conducción de operaciones de información.
- Dispersar las fuerzas, armas y fuegos del enemigo, logrando al mismo tiempo la concentración de las fuerzas, armas y fuegos de las unidades propias.
- Confundir, efectuar diversión o transmitir información falsa al enemigo y persuadirlo de que lo real es falso y lo falso es real.
- Cambiar los datos en las redes.
- Diseminar propaganda.
- Divulgar información redundante.
- Obtener información.

Por su parte, la exploración cibernética consiste en acciones de búsqueda o de colección en los Sistemas de Tecnología de la Información de interés, a fin de obtener la situación del ambiente cibernético. Esas acciones deben preferentemente evitar el rastreo y servir para la producción del conocimiento o identificar las vulnerabilidades de esos sistemas.

Un ejemplo de ello, revelado en *WikiLeaks*, es "un programa de vigilancia conjunta, entre la Agencia de inteligencia de los Estados Unidos (*National Security Agency - NSA*) y la Agencia de inteligencia británica GCHQ (Cuartel General de Comunicaciones del

110 Doutrina Militar de Defesa Cibernética - MD31- M-07 (1ª Edição /2014) de la República Federativa de Brasil. P. 18/36; Disponible en: http://www.defesa.gov.br/arquivos/legislacao/emcfa/publicacoes/doutrina/md31_m_07_defesa_cibernetica_1_2014.pdf.

111 López, Claudio C., "La Guerra Informática", Boletín del Centro Naval, Número 817, Mayo/ agosto de 2007; Disponible en: http://www.centronaval.org.ar/boletin/BCN817/817lopez.pdf

Gobierno) mediante el cual hackearon, descriptaron y siguieron en vivo videos militares israelíes trasmitidos desde aviones no tripulados y aviones de combate"[112].

Según Pierluigi Paganini[113] algunos documentos liberados por el ex contratista de la NSA Edward Snowden revelaron[114] que en una operación llamada a *"Anarchist"*, iniciada en 1998, "el Reino Unido y funcionarios de inteligencia estadounidenses tuvieron acceso de manera habitual a las cámaras de los drones israelíes, lo cual les permitió ver videos en vivo trasmitidos desde aviones no tripulados y aviones de combate mientras Israel bombardeaba Gaza y espiaba a Siria".

Para el Departamento de Defensa de los Estados Unidos[115], las operaciones en el espacio cibernético pueden entenderse como aquellas operaciones que implican "el empleo de capacidades en el espacio cibernético donde el propósito principal es lograr objetivos en o a través del espacio cibernético. Las ciberoperaciones implican el uso de cibercapacidades como equipos, herramientas de software o redes; y tienen un propósito primario de lograr objetivos o efectos en o a través del espacio cibernético".

Para los Estados Unidos de América, tomando como base lo establecido por el *US. Cyber Command* (USCYBERCOM)[116], las operaciones cibernéticas constan de tres líneas diferentes: operaciones de red del Departamento de Defensa, operaciones de espacio cibernético defensivas y operaciones de espacio cibernético ofensivas. El área de operaciones de red del Departamento de Defensa[117] (DODIN) incorpora actividades para diseñar, construir, configurar, asegurar, operar y mantener, así como sostener redes del Departamento de Defensa con el fin de crear y preservar la seguridad de la información en las redes de información de dicho Departamento. El área de operaciones defensivas en el espacio cibernético (DCO) consiste en operaciones pasivas y activas en el espacio cibernético que pretenden preservar la capacidad de utilizar las capacidades del espacio cibernético y proteger datos, redes y capacidades centradas en redes. El área de operaciones ofensivas (OCO) incorpora todas las operaciones realizadas para proyectar el poder contra adversarios en o a través del espacio cibernético.

---

112 Khandelwal, Swati; "How Spy Agencies Hacked into Israeli Military Drones to Collect Live Video Feeds"; Disponible en: http://thehackernews.com/2016/01/drones-hacking.html

113 Paganini, Pierluigi; Anarchist operation, US and UK spied on Israeli UAVs and fighter jets; Disponible en: http://securityaffairs.co/wordpress/44058/intelligence/anarchist-operation-espionage.html;

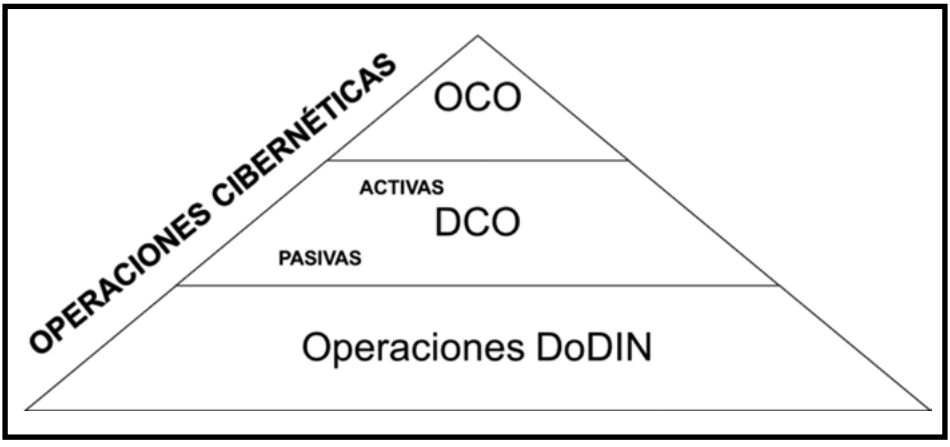
114 Los documentos revelaron que la Agencia de inteligencia británica instaló sistemas de interceptación militares en un complejo de la Royal Air Force en las montañas de Troodos (Chipre), muy cercana geográficamente de Israel y Siria.

115 US Department of Defense, Law of War Manual, Office of General Counsel Department of Defense, June 2015; P. 995 Disponible en: http://archive.defense.gov/pubs/law-of-war-manual-june-2015.pdf

116 Sutton, Walter S.; Lieutenant Colonel; Cyber Operations and the Warfighting Functions; USAWC Strategy Research Project; United States Army; Disponible en: www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA590297.

117 DODIN es un conjunto globalmente interconectado de principio a fin, de capacidades de información para recoger, procesar, almacenar, difundir y administrar información a demanda a los combatientes, autoridades y personal de apoyo.

FIGURA 2: LAS OPERACIONES CIBERNÉTICAS[118]



Para explicar mejor esta organización, en la figura 2 pueden observarse tres conjuntos separados uno de otro, cada uno de los cuales constituye una línea de operación diferente. La primera, la de las Operaciones DODIN, es donde el US *Cyber Command* diseña, construye, configura, asegura, opera, mantiene y sostiene el entorno de información que le fuera asignado para las operaciones. Las operaciones se realizan de forma proactiva e incluyen acciones enfocadas en las TIC, es decir en hardware, software, datos, usuarios individuales y los administradores del sistema. Los ejemplos incluyen corrección de vulnerabilidades conocidas, cifrado de datos como también asegurar que el usuario y el administrador se encuentren capacitados y cumplan con las normas establecidas. Encaran a la seguridad desde la perspectiva de las TIC y no están focalizadas en una amenaza específica. Las operaciones buscan establecer un nivel de seguridad contra actividades maliciosas en el espacio cibernético, incluidas las amenazas internas.

Según la perspectiva del Director de Operaciones del U.S. Cyber Command, Maj. Gen. Brett T. Williams[119] "La naturaleza constantemente cambiante del espacio cibernético, el bajo costo que les significa ingresar a las redes a los actores maliciosos y el gran beneficio potencial para los ciberdelincuentes, hacktivistas o estados-nación significa que se debe hacer mucho más que establecer contraseñas de 15 caracteres de largo. Los comandantes deben priorizar los recursos para cumplir lo más posible las directivas de seguridad".

La segunda línea de operación implica para el US *Cyber Command* defender las operaciones cibernéticas a través de acciones que pueden ser activas o pasivas. Para ello, debe tener la posibilidad de descubrir, detectar, analizar y mitigar las amenazas, lo que incluye

118 Libicki, Martin C. The Convergence of Information Warfare, Strategic Studies Quarterly, Volume 11 Issue 1 - Spring 2017 Figura adaptada por los autores Disponible en: http://www.airuniversity.af.mil/SSQ/

119 Williams, Brett T., The Joint Force Commander's Guide to Cyberspace Operations; Op. Cit.

amenazas internas. En contraposición a las Operaciones de DODIN, las operaciones DCO tienen una misión que cumplir y se enfocan sobre una amenaza específica. Vinculando las vulnerabilidades con la intención y capacidad del adversario, se identifican las áreas de riesgo primario sobre las que se deberán enfocar los esfuerzos defensivos.

Como puede apreciarse en la figura 2, estas operaciones defensivas se subdividen en dos categorías: las medidas defensivas internas y las respuestas activas. Las primeras son aquellas acciones que se toman internamente en el propio espacio cibernético y las otras se toman fuera del entorno propio de información para detener o bloquear un ataque, de la misma manera en que en una operación convencional alguien decide atacar para defenderse, en lo que se conoce en la guerra convencional como un "ataque de desarticulación".

A los fines del adiestramiento, se necesita disponer de la capacidad de poder simular una oposición y de personas capaces de evaluar las vulnerabilidades de las redes propias y asesorar a los administradores de la red, o a los comandantes, en lo que tiene sentido asumir riesgos en función de las misiones operacionales asignadas.

La tercera línea de operación son las OCO en el espacio cibernético que ofrecen una variedad de efectos fuera de las propias redes, para satisfacer las necesidades de la seguridad nacional.

Para los Estados Unidos de América, mientras que las misiones militares en el espacio cibernético (operaciones OCO, DCO y DODIN) se categorizan por intenciones, estas operaciones a su vez requieren del empleo de diferentes capacidades para crear los efectos específicos en el espacio cibernético. Para planificar, autorizar y evaluar estas acciones es importante comprender cómo se distinguen unas de otras[120].

1. **Defensa del espacio cibernético.** Son las acciones que normalmente se originan dentro del espacio cibernético del Ministerio de Defensa para asegurar, operar y defender la DODIN. Estas acciones específicas incluyen proteger, detectar, caracterizar, contrarrestar y mitigar. Tales acciones defensivas son creadas generalmente por el Comandante Conjunto o por la Fuerza Armada específica que posee u opera la red, excepto en ciertos casos en los que estas acciones defensivas afectarían las operaciones de redes fuera de la responsabilidad de la Fuerza Conjunta o de la respectiva Fuerza Armada específica.

2. **Ataque en el espacio cibernético.** Acciones que crean varios efectos directos de negación del espacio cibernético (es decir, degradación, interrupción o destrucción) y la manipulación que conduce a la negación que se encuentra oculta o que se manifiesta en los dominios físicos. Estas acciones específicas son efectos descriptos como:

   a. **Negar:** Degradar, interrumpir o destruir el acceso a, operación de, o disponibilidad de un objetivo por un nivel especificado durante un tiempo especificado. La negación le impide al adversario el uso de los recursos.

---

120 US Department of the Army, Joint Publication 3-12 (R) Cyberspace Operations; 5 February 2013, passim; Disponible en: http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf

i. **Degradar:** Negar el acceso (una función de la cantidad), u operación de un objetivo a un nivel representado como un porcentaje de capacidad. Se debe especificar el nivel de degradación. Si se requiere un tiempo específico, este debe ser especificado.

ii. **Interrumpir:** Negar completamente durante un lapso (función del tiempo) el acceso a, o la operación de un objetivo durante una determinada cantidad de tiempo. Normalmente, debe especificarse el tiempo de inicio y de finalización. La interrupción puede ser considerada un caso especial de degradación en la que el nivel de degradación seleccionado es del ciento por ciento.

iii. **Destruir:** Permanentemente, completamente e irremediablemente negar (las funciones de tiempo y cantidad son maximizadas) el acceso a, o la operación de un objetivo.

b. **Manipular:** Controlar o cambiar la información del adversario, sistemas de información y/o redes de tal manera que apoyen los objetivos del Comandante.

La degradación o destrucción de la capacidad de las redes y los sistemas informáticos enemigos puede realizarse de forma temporal, como pueden ser ataques de red DoS y DDoS, o suponer una degradación más permanente, como por ejemplo, el borrado de sistemas, cambio de configuraciones o corrupción de datos almacenados.

La publicación JP 3-12[121] establece que "La ejecución exitosa de operaciones cibernéticas requiere el empleo integrado y sincronizado de las operaciones ofensivas, defensivas y DODIN, sostenidas por la eficaz y oportuna preparación operacional del medio ambiente".

La preparación operacional del ambiente ciberespacial [122]

Consiste en la habilitación de actividades de no inteligencia llevadas a cabo para planear y prepararse para potenciales operaciones militares sucesivas. Requieren de fuerzas formadas a un nivel que impida las interferencias con operaciones de inteligencia. Se llevan a cabo bajo órdenes de autoridades militares y deben ser coordinadas con otras agencias y departamentos del gobierno.

Para la publicación JP 3-12[123], las acciones de Inteligencia, Vigilancia y Reconocimiento del espacio cibernético son llevadas a cabo por el Comandante Conjunto autorizadas por una Orden Ejecutiva o por unidades de Inteligencia de Señales (SIGINT) bajo control operacional delegado para reunir inteligencia que pueda ser requerida para

121 JP 3-12, Cyberspace Operations, 5 February 2013, P. vii.

122 Ibidem. P. II-5

123 Ibidem. 118, P. II-4

apoyar futuras operaciones, lo que incluye OCO o DCO. Estas actividades deben estar sincronizadas e integrar el planeamiento y la operación de los sistemas del espacio cibernético, en apoyo directo de las operaciones actuales y futuras. Se basan en la inteligencia operacional y táctica y en el mapeo del espacio cibernético del adversario con el fin de apoyar el planeamiento militar. Requieren evitar interferencias mutuas con la comunidad de inteligencia y que las fuerzas del espacio cibernético estén capacitadas y certificadas con un estándar común con la comunidad de inteligencia. Se llevan a cabo bajo órdenes de autoridades militares y deben ser coordinadas con otras agencias y departamentos del gobierno.

De manera coincidente, Leed[124] explica que:

> Las operaciones cibernéticas también incluyen actividades de inteligencia, vigilancia y reconocimiento (Cyber ISR) y de preparación operacional del medio ambiente (Cyber OPE). Las primeras se concentran en la recopilación de información en los sistemas de un determinado adversario e incluyen sus configuraciones de hardware y software, personal y seguridad operacional. Esta información es fundamental para la eficaz orientación, planificación operativa y para determinar las capacidades ofensivas para lograr los efectos deseados. Cyber OPE, por su parte, se centran en el acceso a un sistema de blanco y en los medios específicos de preparación para la operación. El acceso al sistema de blanco está generalmente restringido por defecto, así que resulta necesario disponer de conocimientos avanzados y actualizados del sistema de blanco para garantizar el acceso presente y futuro.

Esto coincidiría con lo que otros países como Brasil, España y Francia que, como ya fuera dicho, denominan operaciones de exploración o explotación (según sea el idioma de donde se traduzca), pues para estos países, la exploración cibernética tiene como finalidad producir conocimiento e inteligencia y, en especial, obtener datos y detectar debilidades y vulnerabilidades. Es lo que frecuentemente la prensa llama *recorrido de las redes.* Técnicamente, es posible detectar cuándo una red está siendo *recorrida* por alguien.

Para Brasil[125], la exploración cibernética consiste en acciones de búsqueda en los sistemas de tecnología de la información de interés, con el fin de obtener datos no autorizados para la producción de conocimiento o identificar las vulnerabilidades de dichos sistemas; el ataque cibernético que comprende las acciones para interrumpir, negar, degradar, corromper o destruir la información almacenada en dispositivos y redes de computadoras y comunicaciones del oponente; y la protección cibernética que abarca las acciones para contrarrestar los ataques cibernéticos y la explotación contra los dispositivos de computadoras y redes de computadoras y comunicaciones

124 Leed, Maren, "Offensive Cyber Capabilities at the Operational Level: The Way Ahead"; Disponible en: https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/130916_Leed_OffensiveCyberCapabilities_Web.pdf

125 Ministerio de Defensa de Brasil, Doutrina de Operações Conjuntas – MD30-M-01 / Volumes 1, P. 56/128, Año 2011; Disponible en: http://www.defesa.gov.br/arquivos/legislacao/emcfa/publicacoes/doutrina/md30_m_01_volume_1.pdf

propios, lo que incrementa las acciones de seguridad cibernética ante una situación de crisis o conflicto armado.

En Estados Unidos, las operaciones de exploración cibernética también reciben el nombre de "operaciones de acceso a medida" (*Tailored Access Operations*) pues como su nombre lo indica, se construyen herramientas de ataque que se ajustan a la medida de sus objetivos como, por ejemplo, se desarrollan modelos de software para irrumpir en marcas y modelos comunes de *"routers, switches y firewalls* de múltiples líneas de proveedores de productos"[126]. Los implantes que crean persisten en el tiempo a través del software y permiten copiar los datos almacenados, recolectar comunicaciones e introducirse en otras redes. Estas operaciones solo serían llevadas a cabo por la *National Security Agency* (NSA).

Al igual que Brasil, España establece que las acciones que comprenden las ciberoperaciones pueden ser agrupadas en cuatro elementos, a saber: ciberoperaciones de red, cibercombate, ciberapoyo y conocimiento de la cibersituación.

En cuanto al cibercombate, Brasil considera que esta emplea básicamente tres elementos o conjunto de acciones: ciberexplotación, ciberataque y ciberdefensa. Las funciones más típicas del componente cibercombate de las ciberoperaciones son: recoger y analizar los datos de redes, sistemas y servicios; estudiar y caracterizar las amenazas; identificar, seguir y explotar las actividades enemigas; suministrar datos para el propio conocimiento de la cibersituación; conducir la ciberdefensa dinámica; y ayudar en la investigación de ataques para determinar su origen.

Como habrá podido apreciarse, casi todos los países consideran que las operaciones cibernéticas son de carácter defensivo, exploratorio y ofensivo con algunas variantes que son producto de sus propias visiones del espacio cibernético. El segundo axioma[127] dice que hay pocos ajustes que hacer para integrar las operaciones del espacio cibernético dentro del actual proceso de planeamiento.

El tercero señala que existe una necesidad imperiosa de tener operadores del espacio cibernético integrados en las células del J 3 y J 5 dentro del Estado Mayor Conjunto de la Fuerza. Se tiene personal experto en operaciones del espacio cibernético principalmente de personal con antecedentes en inteligencia, comunicaciones y criptografía.

Finalmente, como cuarto principio, indica que la palabra ciber tiene una interpretación ambigua si se usa como prefijo de una palabra compuesta, y se debe acordar que espacio cibernético, en definitiva, significa un dominio hecho por el hombre y un ambiente de información creado para conectar computadoras, fibras ópticas, switches, routers, dispositivos inalámbricos, satélites y otros componentes que permiten mover un enorme flujo de información a gran velocidad. En tal sentido, las operaciones en el espacio cibernético son operaciones de apoyo a las operaciones, de la misma forma que lo son la inteligencia y las comunicaciones en todos los otros dominios.

---

126 Gellman, Barton and Nakashima, Ellen; "U.S. spy agencies mounted 231 offensive cyber-operations in 2011, documents show" Disponible en: https://www.washingtonpost.com/world/national-security/us-spy-agencies-mounted-231-offensive-cyber-operations-in-2011-documents-show/2013/08/30/d090a6ae-119e-11e3-b4cb-fd7ce041d814_story.html.

127 Williams, T. The Joint Force Commander's Guide to Cyberspace Operations; Op. Cit.

Las de defensa, por lo general incluyen las medidas para la prevención, detección, reacción y recuperación frente a ataques, intrusiones, interrupciones u otras acciones hostiles deliberadas, que puedan comprometer la información y los sistemas que la manejan. Las de exploración o explotación (según sea el idioma) son aquellas que permiten la recopilación de información sobre sistemas de información de potenciales adversarios y las de respuesta u ofensivas, aquellas otras que incluyen las medidas y acciones a tomar ante amenazas o ataques.

Capacidades operacionales en la dimensión ciberespacial

Una vez definidas las operaciones cibernéticas, se hace necesario conocer cómo la estructura militar adquirirá los medios y se entrenará para este tipo de operaciones. Parte del desafío en el logro de una capacidad es su integración a un concepto de operaciones ya existente. En pocas palabras, sabiendo cómo una fuerza armada quiere combatir, se determinarán las formas en que se adquirirá el material y se entrenará al personal.

Para Eissa y otros,[128]

> ... debemos tener presente, como indica Ernesto López, que la perspectiva estratégica de la OTAN "se funda en una noción amplia de seguridad, en la que se destacan la complejidad y la multidimensionalidad como asuntos centrales y en un concepto de indivisibilidad de la misma" (López, 2004: 70)[129]. Esta dimensión ampliada de la seguridad incluye a las genéricamente denominadas "nuevas amenazas", razón por la cual los criterios adoptados para este desarrollo de capacidades militares no pueden trasladarse directamente al Sistema de Defensa argentino"[130].

Pese a que la Argentina, así como todos los países de la Organización de Estados Americanos aceptaron en el año 2003 el concepto de seguridad multidimensional[131], al persistir en una postura ideológica según la cual seguridad es sinónimo de seguridad pública interna, y defensa es seguridad pública externa de amenazas de otros militares de otros países, lo cual es inaplicable al espacio cibernético y diferente de los conceptos

---

128 Eissa, Sergio G., Gastaldi, Sol, Poczynok, Iván y Zacarías Di Tullio, María Elina, Op. Cit.

129 López, Ernesto (2004) "Nueva problemática de seguridad y nuevas amenazas", en Ernesto López y Marcelo Saín (comps.) Nuevas amenazas. Dimensiones y perspectivas. Dilemas y desafíos para la Argentina y el Brasil. Bernal: Universidad Nacional de Quilmes.

130 Decreto 727/2006, Reglamentación de la Ley Nº 23.554. Principios Básicos. Competencia del Consejo de Defensa Nacional. Atribuciones del Ministerio de Defensa. Estado Mayor Conjunto de las Fuerzas Armadas. Fuerzas Armadas. Disposiciones Complementarias. Párrafo 11 "que por ello deben rechazarse enfáticamente todas aquellas concepciones que procuran extender y/o ampliar la utilización del instrumento militar hacia funciones totalmente ajenas a la defensa, usualmente conocidas bajo la denominación "nuevas amenazas", responsabilidad de otras agencias del Estado organizadas y preparadas a tal efecto"; Disponible en: http://servicios.infoleg.gob.ar/infolegInternet/anexos/115000-119999/116997/norma.htm

131 Declaración AG/DEC. 27 (XXXII-O/02), Conferencia de Seguridad Hemisférica México 2003, Considerando que la Declaración de Bridgetown reconoce que las amenazas, preocupaciones y otros desafíos a la seguridad en el hemisferio son de naturaleza diversa y alcance multidimensional y que el concepto y enfoque tradicionales deben ampliarse para abarcar amenazas nuevas y no tradicionales, que incluyen aspectos políticos, económicos, sociales, de salud y ambientales.

vigentes en el contexto internacional en general, (la OTAN, Rusia, China, India, Brasil y los restantes estados del mundo), Argentina pareciera querer desechar desde el inicio cualquier cooperación internacional en la defensa del ciberespacio, un espacio sin fronteras geográficas que requiere la integración de esfuerzos estatales.

Para la Directiva de Política de Defensa Nacional 2654/14 a la que se están refiriendo las capacidades operacionales en el espacio cibernético, la ambigüedad genera anfibologías como la que sigue:

> Deberán desarrollarse capacidades operacionales en la dimensión ciberespacial con el objeto de adquirir competencias en los ambientes terrestre, naval y aéreo, así como de ciberseguridad de redes pertenecientes al Sistema de Defensa Nacional y respecto de los objetivos de valor estratégico que oportunamente sean definidos por el Nivel Estratégico Nacional.

Como se ha visto, las crisis que se presentarán en escenarios futuros y más aún en el espacio cibernético serán más complejas que las precedentes, pues deberán enfrentarse amenazas de carácter sutil, multipolar e indefinidas. La inteligencia y la innovación resultarán elementos fundamentales para determinar las soluciones para combatirlas o anularlas.

Es precisamente esta falta de información lo que hace difícil poder responder a la pregunta ¿cuánto es suficiente? Para poder determinarlo, los países en general y, entre ellos la República Argentina,[132] han adoptado como método de planeamiento militar el denominado "planeamiento por capacidades" enfocado no sólo a determinar los medios necesarios para un tipo de conflicto concreto o una misión específica, si no hacia algo mucho más general que permita abarcar un amplio espectro de ellos.

En la Argentina, Uzal, Riesco y otros[133] brindan algunos ejemplos referidos a una aplicación concreta de la planificación basada en capacidades a partir de la evaluación de las amenazas conocidas y del análisis de las vulnerabilidades detectadas contra las capacidades a ser adquiridas, desarrolladas, fortalecidas y ampliadas.

Para estos autores, son ejemplos de capacidades a ser adquiridas las que siguen:

a. **Capacidad de detección de ciber armas,** es decir de malware sumamente sofisticado que no es detectado ni por el software de base ni por los productos anti – malware disponibles hoy comercialmente;
b. **Capacidad de Análisis de Flujo de Redes,** es decir poder identificar a "las fuentes" de un ataque cibernético y diferenciar los computadores "zombies" de los verdaderos Servidores de Comando y Control;

---

132 En la República Argentina, el Decreto 1729/2007 mediante el cual se aprueba el "Ciclo de Planeamiento de la Defensa Nacional" establece que "La aplicación de un modelo de planeamiento de diseño de fuerzas del Instrumento Militar, basado en el desarrollo de capacidades" las cuales "abarcan un conjunto de factores (recursos humanos, material, infraestructura, logística, información, adiestramiento, doctrina y organización), empleados en base a principios y procedimientos doctrinarios.

133 Uzal, Roberto, Riesco, Daniel, Montejano, Germán y Berón, Mario; Planeamiento Estratégico Informático: Planeamiento Basado en Capacidades aplicado al Planeamiento Estratégico de la Ciberdefensa, 7mo Simposio Argentino de Informática en el Estado - SIE 2013; Disponible en: http://42jaiio.sadio.org.ar/proceedings/simposios/Trabajos/SIE/22.pdf

c. **Capacidad de ingeniería reversa de ciber armas;**
d. **Capacidad de Análisis de ciber armas** a partir de contenidos de Bases de Datos/Bases de conocimiento de una futura Agencia de Ciberdefensa utilizando técnicas del tipo Reconocimiento mediante Patrones,
e. **Capacidad de respuesta ante ciber agresiones;**
f. **Capacidad de evitar el uso del territorio propio para lanzar ciber agresiones;**

Todo ello, con el objetivo de:

- Adquirir los conceptos, desarrollar las habilidades y construir las herramientas para lograr la identificación de las arquitecturas tipo de ciber armas (primera alerta de la detección)
- Acceder en lo inmediato a ambientes de simulación de ciber ataques que actualmente estén utilizando países amigos.
- Lograr la integración dinámica de los especialistas en detección de malware de alto nivel de sofisticación a grupos de tipo CERT (*Computer Emergency Response Teams*)
- Desarrollar, con *know how* propio, herramientas de software para asistir en la detección temprana de Ciber ataques de alto nivel de sofisticación (completar lo iniciado con la construcción de las herramientas para lograr la identificación de las *arquitecturas tipo* de ciber armas).

Estas capacidades descriptas parecen más apropiadas para un estado con la tecnología más avanzada en el asunto. Disponer de un software de propio desarrollo para detectar armas cibernéticas pareciera estar fuera del alcance de la tecnología nacional. Si bien sería conveniente poder implementar el propio sistema operativo y desarrollar el propio antivirus y antimalware, hasta tanto se dispongan de las capacidades para ello, se podría hacer como Brasil, que ha firmado acuerdos con la empresa Panda y las universidades para detectar malware en sus sistemas.

Para Acosta[134], el Mando Aliado de Transformación (ACT) de la OTAN, con la finalidad de apoyar una obtención coordinada e interoperable de las capacidades de ciberdefensa entre los países aliados, le encargó a la NC3A[135] "realizar una desglose, clasificación o taxonomía de las capacidades de ciberdefensa, con el objeto de dar una idea clara de sus aspectos operativos y dividir el esfuerzo de desarrollo u obtención en piezas manejables que puedan ser tratadas de forma independiente". Esta clasificación desglosa la ciberdefensa en seis grandes áreas de capacidad, cada una de las cuales, a su vez, se

134 Acosta, Óscar Pastor, Capacidades para la Defensa en el Espacio cibernético, Cuadernos del CESEDEN. P. 214; Disponible en: http://www.defensa.gob.es/ceseden/Galerias/destacados/publicaciones/monografias/ficheros/126_EL_ESPACIO CIBERNÉTICO_NUEVO_ESCENARIO_DE_CONFRONTACION.pdf

135 La NC3A es parte de la estructura C3 de la OTAN, junto con el NATO C3 Board y la NCSA (NATO CIS Service Agency). La misión de la NC3A es facilitar la consecución de los objetivos de la Alianza a través de la prestación imparcial de las capacidades de Consulta, Mando y Control, Comunicaciones, Inteligencia, Vigilancia y Reconocimiento (C4ISR).

divide sucesivamente en otras sub capacidades subyacentes[136], y así hasta llegar a un nivel de detalle suficiente.

a. **Detección de actividad maliciosa:** capacidad que se implementa a través de la recopilación de información de una amplia gama de sensores, base para el análisis que separe los flujos de tráfico entre entidades maliciosos, que permita una evaluación de la situación. Ésta se logra relacionando entidades maliciosas entre sí y con las entidades de origen y destino, además de tener en cuenta el histórico de actividades entre ellas.
b. **Prevención, mitigación y terminación de ataques;**
c. **Análisis dinámico de riesgos, ataques y daños;**
d. **Recuperación de ciberataques:** capacidad para recuperarse de un ataque mediante la restauración del sistema y la información a su estado original y a sus propiedades de seguridad.
e. **Toma de decisiones oportunas:** capacidad de decidir sobre las acciones a ser implementadas de manera oportuna. Dado que en el espacio cibernético los eventos pueden desarrollarse de forma vertiginosa, esto implicará que en muchas ocasiones la respuesta sea automática para garantizar que es suficientemente rápida. En cualquier caso, será preciso la toma de decisiones por humanos para coordinar los resultados de diferentes respuestas y elegir la mejor vía a seguir en el proceso de defensa.
f. **Gestión de la información de ciberdefensa:** capacidad de recopilar y compartir información de forma que permita un intercambio rápido y fiable de esta entre diferentes partes. Entre la información de referencia sobre ciberdefensa a compartir se encontrará una estimación de la intención del adversario y de su capacidad, así como información acerca de las vulnerabilidades conocidas, software malicioso y las evaluaciones y certificaciones de los diferentes productos de software y hardware.

Hecho esto, según el método señalado, correspondería descomponer cada una de las capacidades determinadas en los elementos que la conforman, que no son otra cosa que las letras del acrónimo que la doctrina argentina denomina MIRILADO[137] [138], Material – Infraestructura – Recursos humanos – Información – Logística – Adiestramiento – Doctrina – Organización.

El Jefe del Estado Mayor de la Defensa de España[139], en su *"Concepto de Ciberdefensa Militar"* señala que las capacidades de la ciberdefensa (de defensa, de explotación y de respuesta) deberán ser desarrolladas considerando los siguientes aspectos o dimensiones:

---

136 Acosta, Op. Cit.

137 Estado Mayor Conjunto de las Fuerzas Armadas, Publicación PC 20 – 09 "Planeamiento para la Acción Militar Conjunta Nivel Estratégico Militar", Proyecto, Público, Edición 2008, P. 92.

138 Este sistema de análisis es similar al empleado por otros países y organizaciones Internacionales (DOTMLPF de Estados Unidos), PRICIE canadiense, el australiano FIC/POSTED, etc.) En España se lo conoce por el acrónimo de "MIRADO"

139 Acosta, Op. Cit.

- **Material:** para garantizar la concordancia de los procesos de adquisición de material con la rapidez de los cambios tecnológicos y la adecuación a la normativa de protección de la información, prestando especial atención a las garantías de seguridad de toda la cadena de suministros (del hardware y del software).
- **Infraestructura:** para que las instalaciones y componentes de los sistemas de información y comunicaciones cuenten con las adecuadas medidas de seguridad física y de emisiones electromagnéticas no deseadas.
- **Recursos humanos:** para disponer de personal formado técnicamente y con continuidad adecuada para garantizar la eficacia y la eficiencia de la ciberdefensa, en la que el personal militar podrá ser complementado con personal civil calificado, que forme parte de equipos multidisciplinares en los que se potencien las sinergias.
- **Adiestramiento:** para que el personal esté adecuadamente concientizado e instruido en la seguridad de la información y en la ciberdefensa. Para ello, los ejercicios de ciberdefensa son fundamentales, debiéndose potenciar su realización en el nivel nacional y fomentar la participación en el internacional. Además, se deberán incluir eventos e incidencias de ciberdefensa en todo tipo de ejercicios militares.
- **Doctrina:** puesto que la naturaleza de la ciberdefensa requiere de una doctrina conjunta y alineada con las de la OTAN y la Unión Europea para proporcionar a los mandos las bases tácticas, técnicas y de procedimiento que les permita ejercer su misión de forma eficaz y eficiente.
- **Organización:** para permitir la implementación de una seguridad dinámica en contra de la actual estructura de los sistemas TIC, orientada hacia la protección estática y el ejercicio de las actividades de explotación y respuesta. Además, la necesidad de una dirección, planificación y coordinación centralizada requiere adaptar la organización para alcanzar la adecuada eficacia de las capacidades necesarias.
- **Colaboración pública privada:** para fomentar acuerdos nacionales e internacionales, entre los sectores público y privado que permitan el intercambio de información y una adecuada coordinación de las acciones.

Como ha podido apreciarse, habiéndose detectado las vulnerabilidades y concebidas aquellas capacidades militares que las reduzcan o anulen, ya no será tan importante determinar quién será el agresor o cuándo y dónde atacará los intereses vitales.

El denominado planeamiento basado en capacidades es una de las opciones metodológicas más adecuadas para encarar el planeamiento en un contexto de indeterminación y de incertidumbre. El desafío consiste en adquirir, desarrollar, fortalecer y ampliar capacidades que fácilmente puedan ser asignadas a casos específicos de un muy amplio espectro de amenazas y escenarios peligrosos.

En la Argentina, el planeamiento por capacidades tiene una debilidad: obvia su tamiz por escenarios. Al evitarlos, puede suceder que cuando llegue el momento, las capacidades cibernéticas desarrolladas no satisfagan las necesidades, especialmente si los desarrollos tecnológicos se han hecho "para atrás", y, sobre todo, si desde Argentina el espacio cibernético es utilizado como plataforma de ataques cibernéticos usando *botnets*.

En función de lo que se ha visto hasta ahora, la postura que aquí se sostiene es que a los efectos de poder cumplir con lo dispuesto en la Directiva de Política de Defensa Nacional, será necesario elaborar un proyecto de plan que permita la obtención de una capacidad de Ciberdefensa Militar y que asimismo garantice el libre acceso al espacio cibernético con el fin de cumplir las misiones asignadas a las Fuerzas Armadas, obtener, analizar y explotar la información sobre ciberataques e incidentes en las redes y sistemas de su responsabilidad, y ejercer la respuesta oportuna, legítima y proporcionada ante amenazas.

En cuanto a las capacidades cibernéticas ofensivas, deberá tenerse presente que el software malicioso se define como la combinación de un método de propagación, un *exploit* y una capacidad de carga diseñados para crear efectos. El método de propagación es cualquier medio de transporte desde su origen a un destino, como una unidad *flash drive* o correos electrónicos de *phishing* dirigidos a organizaciones públicas y privadas. Un *exploit* es un fragmento de software, fragmento de datos o secuencia de comandos y/o acciones, utilizada con el fin de aprovechar una vulnerabilidad de seguridad de un sistema de información para conseguir un comportamiento no deseado del mismo. La carga útil es el propósito: el código escrito para alcanzar el final deseado, tal como la cancelación de los datos o la creación de una destrucción física[140].

De igual manera Uzal[141] señala que,

> ...las capacidades cibernéticas se desarrollan como si se tratase de un misil: tiene una carcasa, una espoleta y una carga explosiva útil. Armas cibernéticas, como Stuxnet, análogamente, poseen cuatro módulos básicos en su arquitectura conceptual: el módulo principal ("carcasa") que, en este caso, se había codificado en lenguaje C, el módulo de "propulsión" (se estima que el Stuxnet estaba codificado en lenguaje Python), el módulo de guiado (presuntamente codificado en lenguaje PERL en la misma arma cibernética) y el módulo de la "carga útil" (aparentemente codificado en lenguaje C++).

En síntesis, el definir las capacidades necesarias requiere en primer lugar, ubicar el nivel de la guerra en el cual va a ser empleada. Por ello, la publicación *Cyberspace Operations Concept Capability Plan* 2016-2028[142] señala que las capacidades tienen cuatro elementos básicos: organización (quién), la idea principal (qué), el medio ambiente, los parámetros y las condiciones (dónde y cuándo) y la razón (por qué). El "quién", identifica el nivel en el que la capacidad es requerida.

---

140 Herr, Trey and Herrick, Drew, Military Cyber Operations: A Primer, The American Foreign Policy Council Defense Technology Program Brief, January 2016, Washington DC, # 14; Disponible en: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2725275

141 Uzal, Roberto – Conferencia en la EST / AFCEA – C.A.B.A. – 27 de junio de 2013 Defensa Cibernética: Panorama global, singularidades del marco regional y propuestas de lineamientos en el ámbito nacional.

142 US Army; TRADOC Pamphlet 525-7-8; Cyberspace Operations Concept Capability Plan 2016-2028; 22 February 2010; Disponible en: https://fas.org/irp/doddir/army/pam525-7-8.pdf

Podrá pensarse que adquirir la capacidad de acceder a determinadas redes, sistemas o nodos, hardware y software del adversario, de manera remota o directa, podría ser el primer y más importante requisito para llevar a cabo operaciones cibernéticas ofensivas o de defensa activa.

Otras capacidades podrían ser las de:

- Acceder, recopilar y explotar la información del adversario para detectar, impedir, negar y neutralizar sus acciones y su libertad de acción.
- Obtener una capacidad de detección automatizada de intrusiones y ataques para detectar, impedir, negar y neutralizar las acciones del adversario, integrar la defensa, asegurar la propia libertad de acción y negar la del adversario en el tiempo y el lugar que se elija.
- Ubicar y entender las estructuras de red del adversario y otras que se especifiquen, para permitir llevar a cabo operaciones cibernéticas.
- Mitigar o evitar medidas defensivas de adversario para poder ejecutar las operaciones cibernéticas.

Lo que no debe dejarse de tener en cuenta es que la determinación de capacidades cibernéticas no solo implica la adquisición de medios, sino que tiene otras implicancias tales como:

- ¿Cómo se desarrollará la doctrina en función de la continua evolución del ciberespacio? ¿Cuáles serán los diseños de organización más eficaces para la ejecución de las operaciones cibernéticas de cada una de las fuerzas armadas, del Comandante Conjunto de Ciberdefensa y del Comandante del Teatro de Operaciones?
- ¿Cuál sería el equilibrio más adecuado entre el adiestramiento conjunto y el específico de cada fuerza armada, para el personal que lleva a cabo operaciones cibernéticas?
- ¿Cómo se forman conductores que comprendan el ciberespacio y las operaciones cibernéticas y que sepan integrar y utilizar las operaciones cibernéticas en el amplio espectro de las operaciones militares?
- ¿Cómo se logrará la compatibilidad y la interoperabilidad de los sistemas de operaciones cibernéticas entre las fuerzas armadas?
- ¿Qué tecnologías son fundamentales para considerar e invertir, para el desarrollo de soluciones efectivas en materia de operaciones cibernéticas?
- ¿Cuáles son las asociaciones público-privadas necesarias para desarrollar las capacidades cibernéticas?

Ciberdefensa y Ciberseguridad

Para la Directiva de Política de Defensa Nacional 2654/14, deberá entenderse como Ciberdefensa a “las acciones y capacidades desarrolladas por el Instrumento Militar

en la dimensión ciberespacial de carácter transversal a los ambientes operacionales terrestre, naval y aéreo".

Para Eissa[143] y otros,

> ... sólo una porción de estas operaciones (cibernéticas) afecta específicamente el ámbito de la Defensa Nacional. En este sentido, entendemos que, dentro de la amplia gama de operaciones cibernéticas, únicamente son de interés para la Defensa Nacional aquellas que persiguen objetivos militares; es decir, que poseen la intención de alterar e impedir el funcionamiento de las capacidades del Sistema de Defensa Nacional. Por lo tanto, aquellas agresiones que afecten toda otra infraestructura que no pertenezca al Sistema de Defensa Nacional son responsabilidad, en primera instancia, de otras agencias del Estado; mientras que aquellos ataques que afectan la capacidad operativa del Instrumento Militar y sus redes requieren la participación del Sistema de Defensa Nacional.
>
> En este contexto, proponemos avanzar en una dirección que permita al Sistema de Defensa Nacional, a partir de sus competencias jurisdiccionales, contribuir a la ciberseguridad en un sentido general o ampliado, coordinando su accionar con otras entidades y jurisdicciones del Sector Público Nacional, a la vez que desarrollar y fortalecer las capacidades de ciberdefensa a fin de estar en condiciones de efectuar una defensa indirecta[144] en el ciberespacio contra un agresor militar estatal externo que pudiera atacar convencionalmente a nuestro país.

No obstante y contradictoriamente, para el principal socio de la Argentina en UNASUR y MERCOSUR, la República Federativa de Brasil, según el General de Brigada del Ejército Brasilero Paulo Sergio Melo de Carvalho, la Ciberdefensa es un "Conjunto de acciones defensivas, ofensivas y exploratorias, llevadas a cabo en el espacio cibernético, en el contexto de una planificación de nivel estratégico nacional coordinado e integrado por el Ministerio de Defensa, para los fines de proteger los sistemas de información del país, obtener datos para la producción de conocimiento de inteligencia y comprometer la eficacia de los sistemas de información del adversario[145]".

Para el Reino de España, en consonancia con la Estrategia de Seguridad Nacional de 2013, la Estrategia de Ciberseguridad Nacional[146] establece que la Ciberdefensa en las fuerzas armadas debe: "Potenciar las capacidades militares y de inteligencia para ejer-

---

143 Eissa, Sergio G., Gastaldi, Sol, Poczynok, Iván y Zacarías Di Tullio, María Elina, Op. Cit.

144 En el mundo se habla de defensa pasiva.

145 Melo de Carvalho, Paulo Sergio, Defesa Cibernética e as Infraestruturas Críticas Nacionais, Anais Do X Ciclo De Estudos Estratégicos: Proteção Das Infraestruturas Críticas, Disponible en: http://www.eceme.ensino.eb.br/meiramattos/index.php/RMM/issue/view/15 El subrayado es nuestro

146 España, Estrategia de Ciberseguridad Nacional, Año 2013 Disponible en: http://www.lamoncloa.gob.es/documents/20131332estrategiadeciberseguridadx.pdf

cer la respuesta oportuna, legítima y proporcionada en el espacio cibernético ante amenazas o agresiones que puedan afectar a la Defensa Nacional".

Consecuentemente con ambos documentos, la Orden Ministerial 10/2013[147] por la que se crea el Mando Conjunto de Ciberdefensa de las Fuerzas Armadas del Reino de España define Ciberseguridad como "el conjunto de actividades dirigidas a proteger el espacio cibernético contra el uso indebido del mismo, defendiendo su infraestructura tecnológica, los servicios que prestan y la información que manejan".

Dicha Orden Ministerial define a la Ciberdefensa militar como el "Conjunto de recursos, actividades, tácticas, técnicas y procedimientos para preservar la seguridad de los sistemas de mando y control de las Fuerzas Armadas y la información que manejan, así como permitir la explotación y respuesta sobre los sistemas necesarios, para garantizar el libre acceso al espacio cibernético de interés militar y permitir el desarrollo eficaz de las operaciones militares y el uso eficiente de los recursos."

Para la República de Colombia[148], Ciberdefensa es la "capacidad del estado para prevenir y contrarrestar toda amenaza o incidente de naturaleza cibernética que afecte la soberanía nacional" y Ciberseguridad es la "capacidad del estado para minimizar el nivel de riesgo al que están expuestos sus ciudadanos, ante amenazas o incidentes de naturaleza cibernética."

Para la International Society[149], ciberseguridad

> ...es un término amplio y algo impreciso al que diferentes actores utilizan con diferentes significados, entre ellos "seguridad informática y seguridad de la información", seguridad de la infraestructura de Internet, seguridad de todo lo que esté conectado a Internet (incluidos los "servicios esenciales" como la distribución eléctrica), seguridad de los datos, aplicaciones y comunicaciones, seguridad de los usuarios de Internet (particularmente de los niños), y con frecuencia abarca nociones tanto de seguridad "nacional" como de seguridad "privada". De hecho, no hay un consenso generalizado con respecto al significado de este término.

Esta imprecisión la explica Julio César Ardita, quien expresa que el término ciberseguridad fue evolucionando a partir de 1965 cuando el Departamento de Defensa de los Estados Unidos comenzó a proteger sus sistemas de cómputos. En 1983, la información pasó a ser encriptada y la aparición, en 1985, de los primeros virus, dio lugar a que en

---

147 Ministerio de Defensa, España, Orden Ministerial 10/2013 de 19 de febrero; Disponible en: http://www.ieee.es/Galerias/fichero/Varios/BOD_26.02.2013_MandoConjuntoCiberdefensa.pdf o bien en http://www.emad.mde.es/Galerias/MOPS/novoperaciones/multimedia/documentos/20130226_CIBERDEFENSA.pdf

148 República de Colombia, "Lineamientos de Política para Ciberseguridad y Ciberdefensa", 14 de julio de 2011. La Política Nacional de ciberseguridad y ciberdefensa involucra a todos los sectores de la sociedad, bajo el liderazgo del Ministerio de Defensa Nacional y en coordinación con las demás entidades del Estado; Disponible en: https://www.unodc.org/res/cld/lessons-learned/col/lineamientos-de-politica-para-ciberseguridad-y-ciberdefensa_html/Lineamientos_de_politica_para_ciberseguridad_y_ciberdefensa.pdf

149 Internet Society, Seguridad y resiliencia de Internet, sitio web Disponible en: http://www.Internetsociety.org/sites/default/files/BPSecurity_Resilience-SPAN_0.pdf

1990 se estableciera la denominada "seguridad en sistemas operativos y redes", en 2000 se hablaba de "Seguridad Informática General", en 2009, de Seguridad de la Información y finalmente, de "Ciberseguridad"[150].

Internacionalmente, existe una definición de ciberseguridad dada por la Unión Internacional de Telecomunicaciones en su Resolución 181, Recomendación UIT - TX.1205 de noviembre de 2010, organismo que en la Conferencia de Guadalajara adoptó la siguiente:

> La ciberseguridad es el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno. Los activos de la organización y los usuarios son los dispositivos informáticos conectados, los usuarios, los servicios/aplicaciones, los sistemas de comunicaciones, las comunicaciones multimedios, y la totalidad de la información transmitida y/o almacenada en el ciberentorno. La ciberseguridad garantiza que se alcancen y mantengan las propiedades de seguridad de los activos de la organización y los usuarios contra los riesgos de seguridad correspondientes en el ciberentorno. Las propiedades de seguridad incluyen una o más de las siguientes: 1) disponibilidad; 2) integridad, que puede incluir la autenticidad y el no repudio; y 3) confidencialidad[151].

Para Melo de Carvalho[152], la Seguridad Cibernética

> ...es un término que se refiere a la protección y garantía de la utilización de activos de información estratégica, especialmente aquellos vinculados a infraestructuras críticas de información (redes de computadoras y comunicaciones y sus sistemas computarizados) que controlan las infraestructuras críticas nacionales. También abarca la interacción con organismos públicos y privados involucrados en la operación de las infraestructuras críticas nacionales, especialmente los órganos de la Administración Pública Federal.

Para la República de Francia[153], la publicación *Les systèmes d'information et de communication (SIC) en opérations,* define:

---

150 Ardita, Julio César Los desafíos de la ciberseguridad y la ciberdefensa, Segurinfo Argentina 2016, Diponible en: http://www.cybsec.com/upload/Ardita_Arias_Segurinfo_AR_2016_Ciberseguridad.pdf

151 Unión Internacional de Telecomunicaciones (UIT), Ciberseguridad, Documento Disponible en: http://www.itu.int/net/itunews/issues/2010/09/20-es.aspx.La Unión Internacional de Telecomunicaciones (UIT) es el organismo especializado en telecomunicaciones de la ONU, encargado de regular las telecomunicaciones a nivel internacional entre las distintas administraciones y empresas operadoras. La sede de la UIT se encuentra en la ciudad de Ginebra, Suiza.

152 Herr, Trey and Herrick, Drew Op. Cit.

153 Centre interarmées de concepts, de doctrines et d'expérimentations, Les systèmes d'information et de communication (SIC) en opérations, Doctrine interarmées DIA-6_SIC-OPS (2014) N° 147/DEF/CICDE/NP du 24 juin 2014 Amendée le 16 janvier 2016, P. 71 t 72; Disponible en: http://www.cicde.defense.gouv.fr/IMG/pdf/20160116_np_dia-6_sic-ops_2014__amendee_janvier_2016.pdf.

Ciberseguridad como el estado buscado por un sistema de información para resistir eventos del espacio cibernético que podrían poner en peligro la disponibilidad, integridad o confidencialidad de la información almacenada, procesada o transmitida y los servicios que estos sistemas ofrecen o hacen disponibles. La Seguridad cibernética se obtiene por la combinación coordinada de la protección de los sistemas de información y su defensa, complementada con las capacidades de resiliencia y restauración de redes y sistemas (ciber-resiliencia).

Ciberdefensa como el ensamble de todas las acciones defensivas u ofensivas conducidas en el espacio cibernético en preparación o en la planificación y realización de operaciones militares, para asegurar la eficacia de la acción de las fuerzas armadas y el funcionamiento del Ministerio. Ella complementa las medidas de protección de redes, de sistemas y de información con una capacidad de poder operar en el espacio cibernético y una capacidad de gestión de crisis cibernética.

La Organización de los Estados Americanos (OEA) estableció una Estrategia Interamericana integral para combatir las amenazas a la seguridad cibernética. Esta fue establecida como un enfoque multidimensional y multidisciplinario dirigido a la formación de una cultura de seguridad cibernética para proteger la infraestructura de las telecomunicaciones, redes y sistemas de información.

En 2005, la Organización de los Estados Americanos (OEA) propició la creación de una Red Interamericana de Seguridad Cibernética constituida a partir de los grupos nacionales de "vigilancia y alerta", también conocidos al presente como los Equipos de Respuesta a Incidentes de Seguridad en Computadoras (CSRITs), teniendo como objetivos identificar y luchar contra las amenazas, independientemente de su origen y motivación; formular planes nacionales de respuestas a situaciones de emergencia; crear una red interamericana de vigilancia y alerta para diseminar rápidamente información sobre seguridad cibernética y responder a crisis, incidentes y amenazas a la seguridad en computadoras.

En 2012, los miembros de la OEA firmaron la declaración de Fortalecimiento de la Seguridad Cibernética de las Américas (2012), y en 2015 el Comité Interamericano contra el Terrorismo (CICTE) de la OEA adoptó la Declaración sobre la Protección de Infraestructura Crítica ante las Amenazas Emergentes. En abril de 2015 se publicó el primer Informe de Seguridad Cibernética e Infraestructura Crítica de las Américas[154].

La información reunida ofrece una importante perspectiva de los ataques cibernéticos sufridos por las organizaciones de infraestructura crítica en la región, así como de las medidas y políticas de seguridad cibernética de las organizaciones; de la colaboración con los gobiernos locales; y de su preparación para enfrentar los ataques cibernéticos.

---

154 Organization of American States. Informe seguridad cibernética e infraestructuras críticas en las Américas 2015; Disponible en: https://www.sites.oas.org/cyber/Certs_Web/OEATrend%20Micro%20Reporte%20Seguridad%20Cibernetica%20y%20Porteccion%20de%20la%20Inf%20 Critica.pdf Disponible en: http://noticiasasis143.blogspot.com.ar/2015/04/informe-seguridad-cibernetica-e.html

En el Resumen Ejecutivo del citado informe, se concluye que[155]:

> Si bien las organizaciones de América han hecho un buen trabajo para proteger la infraestructura crítica contra los ataques, se acerca un punto crítico. Debido a que la frecuencia y la sofisticación de los ataques continuarán o se agravarán y se enfocarán no sólo en afectar a la infraestructura crítica sino también en comprometer la información vital que pudiera usarse en el futuro, los defensores pronto podrían no tener el apoyo necesario para prevenirlos. La falta de financiamiento y de liderazgo gubernamental en esta área deja a los defensores sintiéndose cada vez más solos. Más que eso, los gobiernos de la región necesitan tender la mano a los encargados de la infraestructura crítica que buscan ayuda y guiarlos para ofrecer mejor protección contra los crecientes ataques a este sector crucial.

Como se puede apreciar, al igual que ocurre con los conceptos analizados anteriormente, para el caso de la ciberseguridad y la ciberdefensa tampoco existe un consenso al respecto de lo que significa cada término en particular.

No obstante, podría decirse que ciberseguridad es un conjunto de acciones orientadas a hacer más seguras las redes y sistemas de información que constituyen el espacio cibernético; detectando y enfrentando intrusiones; detectando, reaccionando y recuperándose de incidentes; y preservando la confidencialidad, disponibilidad e integridad de la información. Por su parte, la ciberdefensa como capacidad militar, proviene del incremento en el uso del espacio cibernético para el desarrollo de operaciones militares. Es, por lo tanto, un concepto ligado al principio de libertad de acción y que, al contrario de la ciberseguridad, pretende actuar de forma activa sobre los sistemas de información adversarios.

Nótese que curiosamente, los conceptos de seguridad y defensa en este ambiente son opuestos a los que se sostienen en la Argentina. En la Guerra Fría, seguridad era la condición que permitía que los estados alcanzasen su desarrollo y progreso. Cuando esa seguridad era atacada, intervenía la defensa. Por lo tanto, la defensa era un subconjunto de la seguridad.

En el ámbito cibernético, es exactamente a la inversa. Se requiere de seguridad cibernética en las propias redes y sistemas, y la defensa debe asegurar tal seguridad. Resulta entonces que la seguridad es un subconjunto de la defensa.

En síntesis, la relación entre ciberseguridad y ciberdefensa la señala Celso Perdomo González[156] para quien,

> ...de manera conceptual Seguridad y Defensa conforman un continuo que debe ser gestionado integralmente, pues es evidente que las tecnologías, fundamentalmente las

155 Ibidem P. 7

156 Perdomo González, Celso (Universidad de Las Palmas de Gran Canaria) "Inteligencia y Ciberdefensa; nuevos paradigmas en las Estrategias de Seguridad Nacional." XI Congreso Español de AECPA GT 6.3 Estudios estratégicos y seguridad internacional; Disponible en: http://www.aecpa.es/uploads/files/modules/congress/11/papers/870.pdf

Tecnologías de Información y Comunicaciones que subyacen en esa gestión integral deben ser administradas y consideradas conjuntamente. En el mismo sentido, información, seguridad de la información y la producción de inteligencia en el ámbito de las estrategias de seguridad nacional deben ser tratadas bajo una óptica interdisciplinaria.

Análisis de los términos Internet profunda, gobernanza de Internet y otros conceptos asociados

La Internet profunda

Los acontecimientos han sucedido en forma acelerada, desde que a las 22:30 del miércoles 29 de octubre de 1969, el estudiante Charly Kline de la Universidad de California intentó conectarse con una computadora del Instituto de Investigación de Stanford donde estaba otro estudiante, Bill Duvall. Tenía que transmitir la palabra login (conectar) pero la máquina se tildó. Más tarde lo logró, pero lo que se transmitió fue la palabra logon, por error. Ese fue el origen de Internet.

En 1961, Leonard Kleintrock publicó un análisis sobre la posibilidad de transmitir información en forma de paquetes de datos, es decir no en un solo paquete o bloque. Pensaba que, de esa manera, se podían aprovechar las redes de comunicaciones existentes. Esta posibilidad se exploró por una debilidad militar propia de la Guerra Fría.

Se pensaba que, en caso de un ataque nuclear sobre Washington, la cadena de comando se interrumpiría y la única forma de evitarlo sería aprovechando las redes existentes en el mundo. Kleintrock se dio cuenta de que había una diferencia entre la forma en que los humanos usaban una comunicación telefónica, y la forma en que podían hacerlo las computadoras. En los humanos, un tercio de la comunicación era ocupada por el silencio. Lo mismo pasaba con las computadoras que permanecían mucho tiempo esperando una orden para funcionar. Para aprovechar esa capacidad ociosa, lo mejor era que otros usuarios remotos en una misma red pudieran compartir esas capacidades. En 1969 se inició la primera red de computadoras, denominada ARPANET, y en 1972 se comenzó a hablar de crear una Internet, una red-de-redes. Curiosamente, ya existía en el mundo una marca registrada con ese nombre, Internet, en la Argentina, pero era una empresa de venta de ropa interior[157].

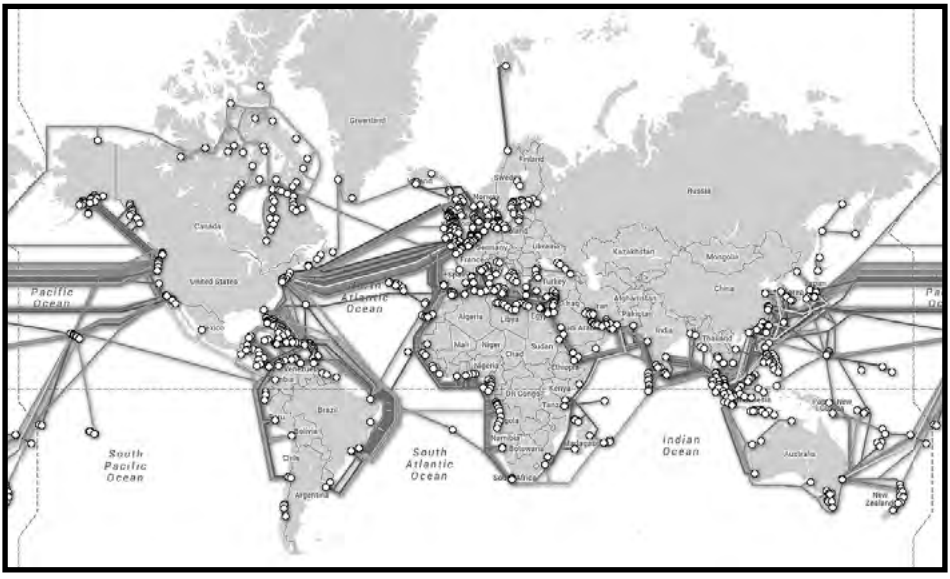
Más de nueve décimas partes del tráfico de Internet viaja a través de cables submarinos de fibra óptica, y estos son agrupados en algunos puntos de bifurcación, por ejemplo, alrededor de Nueva York, el Mar Rojo o el estrecho de Luzón en las Filipinas. El tráfico de Internet está dirigido por 13 clusters de servidores de nombres de dominio[158] potencialmente vulnerables.

---

157 Diario La Nación, Una gran familia llamada Internet; Disponible en: www.lanacion.com.ar/468808

158 El sistema de nombres de dominio (DNS, por sus siglas en inglés, Domain Name System) es un sistema de nomenclatura jerárquico descentralizado para dispositivos conectados a redes IP como Internet o una red privada. Este sistema asocia información variada con nombres de dominios asignados a cada uno de los participantes. Su función más importante es "traducir" nombres inteligibles para las personas en identificadores binarios asociados con los equipos conectados a la red, esto con el propósito de poder localizar y direccionar estos equipos mundialmente.

FIGURA 3: MAPA CONEXIONES FIBRA ÓPTICA[159]



La ciudad bonaerense Las Toninas, a 320 kilómetros de la Capital Federal, fue el lugar elegido por compañías de telecomunicaciones (Telecom, Telefónica, Level 3 y otras) para instalar una de las tecnologías que traen Internet a la Argentina: cables submarinos que dan el acceso al mundo online a través de fibra óptica (aunque no son la única manera en la que el país tiene acceso a la Red)[160].

Para crear una red-de-redes, se necesitaba un lenguaje común que permitiera intercambiar datos. Este lenguaje se llamó TCP (*Transmission Control Protocol*) y luego TCP/IP (*Internetworking protocol*) que provee conectividad de extremo a extremo especificando cómo los datos deberían ser formateados, direccionados, transmitidos, enrutados y recibidos por el destinatario. El modelo TCP/IP y los protocolos relacionados son mantenidos por la Internet *Engineering Task Force* (IETF), una organización internacional abierta creada en Estados Unidos en 1986, que regula las propuestas y los estándares de Internet.

La aplicación del correo electrónico fue ideada por Ray Tomlinson en 1971 y en 1991, Tim Berners creó la *World Wide Web* (www). Así, se permitió el acceso comercial a la red, y en 1995 hubo 16 millones de personas conectadas, en tanto que hoy hay 1669 millones de personas.

159 Bederman, Uriel "Las Toninas: la puerta submarina por la que el país se conecta a Internet". Diario La Nación; jueves 04 de junio de 2015; Disponible en: http://www.lanacion.com.ar/1798446-como-son-los-cables-submarinos-que-traen-Internet-a-la-argentina

160 Ibidem.

En la actualidad, muchas personas utilizan indistintamente los términos Internet y *World Wide Web* (*www*), pero en realidad los dos términos no son sinónimos. Internet y la Web son dos cosas distintas pero relacionadas. Internet es una red masiva de redes, una infraestructura de red. Une millones de computadoras de todo el mundo y forma una red en la que cualquier computadora puede comunicarse con cualquier otro equipo, siempre y cuando ambos estén conectados a Internet.

La *World Wide Web* o simplemente "*la Web*", por su parte, es una forma de acceder a la información por medio de Internet. Es un modelo de intercambio de información que se basa en Internet. La Web usa el Protocolo de Transferencia de Hipertexto (*http*), que es solo uno de los idiomas hablados por Internet, para transmitir datos. Internet, no la Web, también se utiliza para correo electrónico, que se basa en el Protocolo Simple de Transferencia de Correo (SMTP), el grupo de noticias Usenet, mensajería instantánea y *File Transfer Protocol* (FTP). La Web, por lo tanto, es sólo una parte de Internet.

Por último, la Deep Web es, sencillamente, la parte de la Web que está oculta a la vista. Es el contenido de la *World Wide Web* que no forma parte de la Web superficial. No puede accederse por los motores de búsqueda normal. Esta subdivisión masiva de Internet es más de 500 veces más grande que la Web visible. Ha existido desde que las empresas y organizaciones, incluso universidades, pusieron grandes bases de datos en línea de manera que las personas no podían verlas directamente. En lugar de permitir que cualquier persona obtenga números de teléfono de los estudiantes y direcciones de correo electrónico, por ejemplo, muchas universidades requieren a las personas ingresar como miembros de la comunidad del campus antes de buscar directorios en línea para información de contacto.

Dictionary.com[161] define *deep web* como "la porción de Internet que se oculta de los motores de búsqueda convencionales, ya sea por cifrado o por el agregado de páginas web no registradas". Por el contrario, dark web, se define como "la porción de Internet que se oculta intencionalmente de los motores de búsqueda, utiliza direcciones IP enmascaradas y es accesible solamente mediante un navegador web especial". El punto clave aquí es comprender que la *dark web* es parte de la *deep web*.

Lo que ambas tienen en común es que se ocultan de los motores de búsqueda comerciales pues no se puede acceder a ellas a través de, por ejemplo, Google o Bing o Yahoo!.

Cuando las personas discuten sobre los submundos de Internet donde se pueden comprar drogas, armas, pornografía, o contratar asesinos a sueldo - básicamente cualquier artículo o servicio ilícito que se pueda soñar- eso es la *dark web*.

Greenberg[162] observa que mientras que la *deep web* es enorme y representa el 90 y algo por ciento de la Internet, la *dark web* probablemente sólo explica el .01 por ciento. A la *dark web,* a veces denominada *Darknet,* se accede a través de Tor (*The Onion Router*) o I2P (*Invisible Internet Project*)[163] que utilizan direcciones IP enmascaradas para mante-

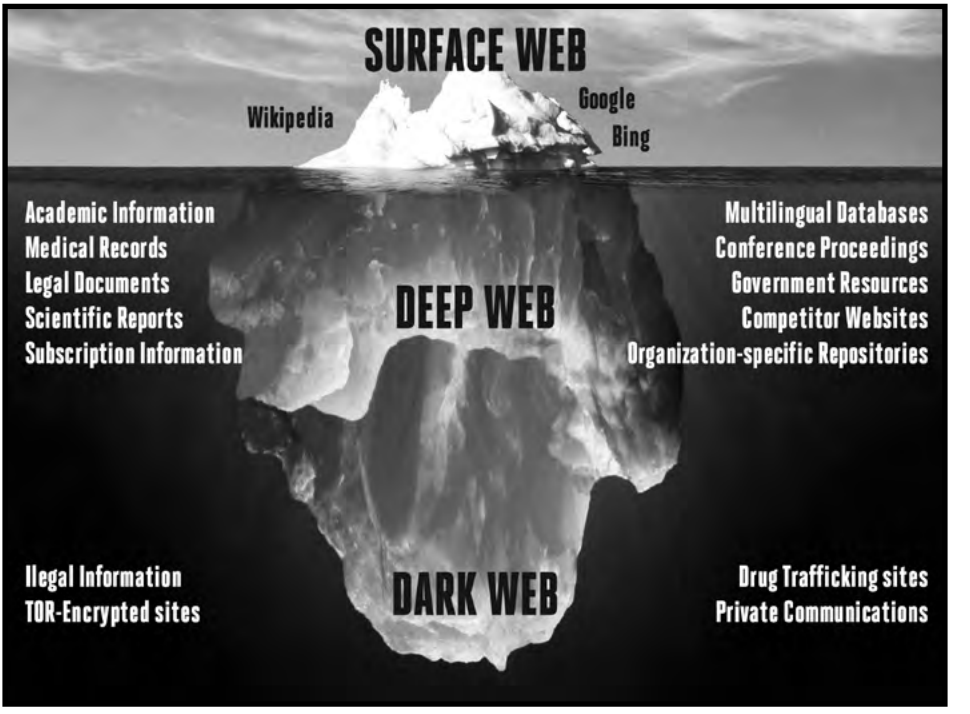
161 Dictionary.com; Disponible en: http://blog.dictionary.com/2015-new-words/

162 Greenberg, Andy, Hackers Lexicon: What is the Dark Web; Wired.com,19 de noviembre 2014; Disponible en: https://www.wired.com/2014/11/hacker-lexicon-whats-dark-web/

163 TOR es un método para comunicarse en línea de forma anónima desarrollado en 2002 por el Laboratorio de Investigación Naval de los EE.UU.,

ner el anonimato de los usuarios y los propietarios del sitio. De esta manera, las personas que utilizan la *dark web* para fines ilícitos no pueden ser rastreadas.

FIGURA 4: LAS DIFERENTES CAPAS DE INTERNET[164]



Ambos sistemas de enrutadores cifran el tráfico web en capas y rebotan a través de computadoras elegidas al azar alrededor del mundo, cada una de las cuales remueve una sola capa de cifrado antes de pasar los datos a su próximo salto en la red. Supuestamente, esto evita que cualquier espía - incluso uno que controla uno de los equipos en la cadena encriptada - pueda hacer coincidir el origen del tráfico con su destino. Cuando los usuarios ejecutan Tor, por ejemplo, los sitios que visitan no pueden ver fácilmente su dirección IP. Pero un sitio web que ejecuta Tor - lo que se conoce como un servicio Tor oculto - sólo puede ser visitado por los usuarios de Tor. El tráfico de la computadora del usuario y el servidor web necesita tres saltos hasta alcanzar el punto de encuentro escogido de forma aleatoria en la red Tor, como si fuera un tráfico anónimo de mercancías en un garaje.

La otra red, I2P, posee muchas de las características de Tor, pero, I2P fue diseñada para ser una red dentro de Internet, con tráfico contenido dentro de sus fronteras. Tor proporciona mejor acceso anónimo a Internet abierto y I2P provee una más robusta y fiable "red dentro de la red"

164 Dark Side of the Web, Subcultures and Deviancy on the Dark Web; Disponible en: https://davidenewmedia.wordpress.com/workingterms/the-surface-web/

La forma en que Tor puede evadir completamente la vigilancia de las agencias como el FBI o las agencias de inteligencia, las cuales disponen de numerosos recursos, sigue siendo una incógnita. Sin embargo, a principios de noviembre de 2014, una acción coordinada por el FBI y Europol conocida como operación *Onymous* permitió incautar decenas de servicios ocultos de Tor, lo que incluyó tres de los seis mercados de drogas más populares en la *Dark Web*.

Según[165] Starr y Crawford, "las autoridades de los Estados Unidos creen que ISIS y otros potenciales terroristas están usando la parte más secreta del mundo online para reclutar combatientes, compartir inteligencia y potencialmente planear ataques reales".

Según les informara un vocero de *Defense Advanced Research Projects Agency* (DARPA), la agencia posee una nueva tecnología militar denominada MEMEX que actúa como un motor de búsqueda único y sigue los patrones de actividad en la Dark Web y sitios web que no están disponibles a través de los enrutadores tradicionales como Google o Bing. "MEMEX permite caracterizar cuántos sitios web existen y qué tipo de contenido hay en ellos".

En síntesis, permanecer escondido en la web se ha convertido en algo fácil de llevar a cabo con herramientas como TOR, un navegador que "rebota" las comunicaciones alrededor del mundo, impidiendo que alguien pueda saber qué sitios visita y dónde se encuentra una persona. Básicamente hace invisible a un usuario.

Para Patrick Tucker[166] "nuevas evidencias sugieren que ISIS o algunos grupos que lo apoyan están buscando el anonimato que les proporciona la Dark Web para ejecutar operaciones más allá de las tradicionales de propaganda que venían llevando a cabo". Según el autor, el Almirante Michael Rogers, Comandante del *U.S. Cyber Command* y director de la *National Security Agency,* cuando daba una conferencia ante el *Cybersecurity for a New America Event* en Washington, dijo que "grupos como ISIS recaudan fondos en la *Dark Web*" y que Ido Wulkan, analista de S2T, una empresa de tecnología con sede en Singapur, recientemente le relevó al periódico israelí *Haaretz* que su empresa había encontrado un número de sitios web de recaudación de fondos para ISIS a través de donaciones de "*bitcoins*"[167].

Según Anthony Cuthbertson[168]

> ...como parte del "proyecto internacional yihad", Wulkan llegó a un sitio de recau-

165 Starr, Barbara and Crawford, Jamie, Pentagon hunts for ISIS on the secret Internet CNN, May 12, 2015; Disponible en: http://edition.cnn.com/2015/05/12/politics/pentagon-isis-dark-web-google-Internet/index.html

166 Tucker, Patrick How the Military Will Fight ISIS on the Dark Web; Disponible en: http://www.defenseone.com/technology/2015/02/how-military-will-fight-isis-dark-web/105948/

167 Bitcoin es una innovadora red de pagos y una nueva clase de dinero que usa tecnología peer-to-peer o entre pares para operar sin una autoridad central o bancos; la gestión de las transacciones y la emisión de bitcoins es llevada a cabo de forma colectiva por la red. Bitcoin es de código abierto; su diseño es público, nadie es dueño o controla Bitcoin y todo el mundo puede participar. Por medio de sus muchas propiedades únicas, Bitcoin permite usos interesantes no contemplados por ningún sistema de pagos anterior.

168 Cuthbertson, Anthony Isis uses bitcoin for fundraising and supporting US-based terror cells 'on both coasts'; Disponible en: http://www.ibtimes.co.uk/isis-uses-bitcoin-fundraising-supporting-us-based-terror-cells-1485670

dación de fondos de ISIS, ligado a un foro turco cerrado. El sitio, sin nombre alguno, contenía el siguiente mensaje de un usuario de nombre Abu Mustafa: "Muchos de nosotros vivimos en los Estados Unidos, y algunos somos prominentes con la comunidad en ambas costas".

Actualmente estamos trabajando con recientemente convertidos al islam y hermanos ya formados que luchan por establecer un nuevo frente islámico en los Estados Unidos y alrededor del mundo." Abu Mustafa pasa a explicar cómo solo las donaciones de bitcoin son aprobadas por la célula, confirmando las sospechas de que ISIS utiliza la moneda encriptada para evitar la detección por los gobiernos occidentales.

Esto no significa que la gente no esté siendo mirada. Según Tucker,

En 2014, una investigación del código fuente en un programa de la NSA llamado XKeyscore, (revelado por las filtraciones de Edward Snowden) demostraba que cualquier usuario simplemente por intentar descargar Tor era automáticamente registrado, lo que permite esencialmente a la NSA conocer la identidad de millones de usuarios Tor. Lo difícil no es encontrar personas que están en la Dark Web, sino que lo arduo es revelar la naturaleza de su interés y su comportamiento dentro de la misma.

No obstante, para el embajador Marc Ginberg[169]:

ISIS y otros grupos del terrorismo islámico radical han convertido a Internet en su propio campo de batalla de los medios de comunicación social. Yihadistas confían en la tecnología de las redes sociales para sobrevivir... es su oxígeno del campo de batalla. Su caja de herramientas es mucho más sofisticada de lo que los americanos puedan imaginar. Utilizando los denominados granjas de servidores ilegales[170] de *dark web*, en Europa oriental y de navegadores seguros, como TOR, que, junto con aplicaciones como *Tunnel Bear*, que estratifican las direcciones IP y eliminan la vigilancia de terceros, ISIS ha podido frustrar las descoordinadas operaciones de inteligencia del mundo occidental. Comunicaciones encriptadas mediante telegramas y WhatsApp agregan más terror a la capacidad de planificación y financiación. Incluso la *National Security Agency* es incapaz de interceptar y descifrar todos los bits de datos que emanan de los conocidos agentes de ISIS. Debemos revertir la ventaja tecnológica de los medios de comunicación social de ISIS. ¿Cómo? Para empezar, nos hemos enfocado demasiado en el cifrado y no en la capacidad del servidor ilícito que sostiene las redes de ISIS. Navegadores seguros que sirven a ISIS están protegidos en Arabia Saudita, Qatar, Turquía, Moldavia y Kosovo. Esa información no es secreta. Nuestra CIA y DIA necesitan más apoyo de la Casa Blanca para abordar el reto de la política exterior que significa atacar esos servidores de ISIS en el extranjero.

169 Ginsberg, Marc, Taking the Fight to ISIS from the Homeland; Disponible en: http://www.huffingtonpost.com/amb-marc-ginsberg/taking-the-fight-to-isis_b_13357798.html

170 Microsoft Azure; Disponible en: https://docs.microsoft.com/es-es/azure/virtual-machines/virtual-machines-windows-sharepoint-farm

En ese artículo, escrito en enero de 2016 y actualizado en diciembre de ese mismo año, el embajador Ginberg señalaba que

> Abdul Razak Ali Artan, un estudiante de la Universidad del Estado de Ohio, nacido en Somalia y criado en Pakistán, (el 28 de noviembre de 2016) embistió con su auto, al estilo ISIS, a un grupo de personas en el campus, al igual que lo ocurrido en Niza, y luego, al estilo del terrorismo palestino, procedió a reducir a sus víctimas con un cuchillo de carnicero que había comprado ese mismo día.

Según informes de prensa el ataque de Artan

> ...fue inmortalizado en una publicación de Facebook en el que el terrorista cita a ISIS como su motivación y a los sermones de YouTube de Anwar al-Awlaki como su inspiración. Horas después del ataque, el New York Times informó que los canales codificados de telegramas dirigido por el estado islámico se refirieron al atacante como "hermano" y utilizaban un hashtag árabe que se traduce como #OhioAttack.

Cuatro meses más tarde, en un artículo de la redacción de la BBC[171] del 24 de marzo de 2017, se señala que:

> Un hombre, identificado el jueves como Khalid Masood -y cuyo nombre de nacimiento era Adrian Russell Ajao embistió con un vehículo, un Hyundai i40 gris, a varios transeúntes en el puente de Westminster, aledaño al Parlamento y al Big Ben. En ese recorrido, Masood mató a dos peatones, una empleada de la escuela de idiomas de 43 años que se dirigía a recoger a sus hijos, y a un estadounidense que se encontraba en Londres con su esposa para celebrar su 25 aniversario de casados. También atropelló e hirió de gravedad a un limpia ventanas de 75 años, quien moriría el jueves en el hospital. Posteriormente, el atacante chocó su vehículo contra una de las vallas que circundan el complejo del Parlamento británico, descendió del mismo y apuñaló a un policía que, pese a los esfuerzos de un parlamentario por salvarlo, falleció.

La nota agrega que: "El agresor luego corrió hacia la entrada del Parlamento y fue abatido por los disparos de agentes no uniformados en la zona conocida como Old Palace Yard" y que "El autodenominado Estado Islámico dijo este jueves que el atacante era uno de sus soldados".

Si bien un reclamo por parte del Estado Islámico al respecto de su responsabilidad en los ataques no prueba que el grupo haya tenido vínculos directos con los ata-

---

171 BBC Mundo. "Ataque en Westminster": claves del atentado que dejó al menos 5 muertos y 50 heridos frente al Parlamento británico en Londres. 25 de marzo de 2017; Disponible en: http://www.bbc.com/mundo/noticias-internacional-39354612

cantes, según Defense News[172], "las autoridades han encontrado que los terroristas tenían lazos digitales".

Para The Times[173],

Khalid Masood estaba usando WhatsApp tres minutos antes de su ataque. La policía trata de establecer lo que el asesino estaba haciendo cuando utilizó el servicio de mensajería WhatsApp cifrado a las 14:37, tres minutos antes de que se subiera a la vereda del puente de Westminster. Las teorías incluyen que estaba diciendo adiós a sus asociados, recibiendo el aliento final o buscando la autorización religiosa antes de atacar.

Jasper Hamill[174] en un artículo denominado: "*ISIS Encyclopedia of Terror: The secrets behind Islamic State's 'information Jihad' on the West revealed*" informó que el *Mirror Online* tuvo acceso a un archivo de material extremista que revela cómo el Estado Islámico recluta, educa y radicaliza a su ejército.

Hamill señala que Mirror online tuvo acceso al caché[175], con lo cual pudo divulgar que el Estado Islámico:

- enseña a los extremistas a ensuciar sus huellas digitales y evitar ser detectados por los servicios de seguridad;
- esto significa que revelan cómo difundir imágenes de atrocidades sin ser rastreados;
- advierte a los extremistas sobre los dispositivos de espionaje que deben divisar, que van desde cámaras escondidas dentro de pequeños relojes hasta finísimos dispositivos de escucha que pueden que ser introducidos en las paredes;
- enseña a los reclutas británicos cómo usar la *dark web* para comunicarse con una red global de terroristas;
- tiene una lista de "*call centers*" con argumentos religiosos prefabricados para utilizar durante los atentados radicales;
- los potenciales reclutas de occidente utilizan una red social rusa para contactarse con extremistas de alto nivel en Siria e Irak.

Frente a ello, Twitter ha tratado de obstruir la presencia de ISIS en su sitio para lo cual ha dictado normas respecto de los contenidos de los mensajes y, desde mediados

---

172 Defense News. London terrorist a 'soldier' of the Islamic State, group claims Disponible en: http://defensenews-alert.blogspot.com.ar/2017/03/london-terrorist-soldier-of-islamic.html

173 The Times; Police search secret texts of terrorist; Disponible en: http://www.thetimes.co.uk/edition/news/police-search-secret-texts-of-terrorist-m6n5lg392

174 Hamill, Jasper, ISIS Encyclopedia of Terror: The secrets behind Islamic State's 'information Jihad' on the West revealed, APR 2015, Updated19:17, 10 AUG 2015; Disponible en: http://www.mirror.co.uk/news/technology-science/technology/isis-encyclopedia-terror-secrets-behind-5528461

175 Caché: memoria de acceso rápido de un microprocesador, que guarda temporalmente los datos recientemente procesados.

de 2015, cerró 360.000 cuentas por violar las políticas de la empresa relacionadas con la promoción del terrorismo[176]. Por tal motivo, los seguidores de ISIS han resuelto el problema de las suspensiones de cuenta simplemente migrando entre plataformas. Para evitar la detección y mitigar los riesgos de seguridad, muchos simpatizantes pasaron de plataformas públicas de base amplia, tales como Twitter o Facebook, a servicios privados de correo electrónico y aplicaciones de mensajería que ofrecen tecnología de encriptación, incluyendo *ProtonMail, Surespot y Telegram.* Debido a la opacidad de estas tecnologías, es difícil medir el número de simpatizantes en cada plataforma. Aun así, en un informe de 2016 titulado *Tech for Jihad*, investigadores Laith Alkhouri y Alex Kassirer escribieron que Telegram ahora "parece ser la mejor opción entre los jihadistas individuales y los grupos jihadistas oficiales".[177]

La *deep Web* - en particular, las redes de la *dark Web* tales como Tor - representa un camino viable para actores maliciosos para el intercambio de bienes, legal o ilegalmente, en forma anónima. El hecho de que muchas actividades no convencionales en la *dark Web* no puedan ser observadas, no significa necesariamente que no existan. De hecho, de acuerdo con el principio que inspira a la *dark Web,* son simplemente más difíciles de detectar y observar. Muchos sitios de la *dark Web* aparecen solo por momentos y después desaparecen, lo cual los hace más difíciles de investigar.

Sumado a ello, Google, Facebook y WhatsApp apoyan a Apple quien se resiste a un fallo judicial que le exigió colaborar para que el FBI desbloqueara el iPhone de uno de los atacantes del tiroteo en San Bernardino, California, en el que el 2 de diciembre murieron 14 personas, aduciendo que la petición es "una medida sin precedentes que pone en peligro la seguridad de nuestros clientes"[178].

Para Michael Chertoff y Tobby Simon [179]

Recientes revelaciones sobre el control a gran escala de Internet por parte de los estado-nación y las recientes detenciones de delincuentes cibernéticos detrás de sitios alojados en la *dark Web* empiezan a conducir a otros cambios. No sería sorprendente ver al ambiente criminal cada vez más fragmentado en *dark webs* alternativas o redes privadas, lo que complica aún más el trabajo de los investigadores. La *dark Web* tiene el potencial para albergar un número cada vez mayor de servicios y actividades maliciosas y, por desgracia, no pasará mucho tiempo antes de que surjan grandes mercados nuevos.

---

176 Alexander, Audrey, How to Fight ISIS Online Why the Islamic State Is Winning on Social Media, April 7, 2017; Disponible en: https://www.foreignaffairs.com/articles/middle-east/2017-04-07/how-fight-isis-online?cid=int-lea&pgtype=hpg

177 Ibidem.

178 Google, Facebook y WhatsApp apoyan a Apple contra el FBI. Clarin.com Sociedad. 18 de febrero de 2016; Disponible en: http://www.clarin.com/sociedad/google-facebook-whatsapp-apple-fbi_0_NyxEL00cg.html

179 Chertoff, Michael and Tobby, Simon The Impact of the Dark Web on Internet Governance and Cyber Security Paper Series: No. 6 — February 2015, Centre for International Governance Innovation and the Royal Institute for International Affairs; Disponible en: https://www.ourInternet.org/sites/default/files/publications/GCIG_Paper_No6.pdf

Un ejemplo de esta fragmentación lo explican Alkhouri y Kassireren[180] quienes, en un trabajo de su autoría titulado *Tech for Jihad,* examinaron las fuentes primarias de la *Deep* y la *Dark Web* para identificar y analizar las principales tecnologías digitales que facilitan la proliferación de agendas radicales de actores como ISIS.

Además de TOR, los miembros del Estado Islámico han comenzado a usar otro navegador de internet llamado Opera Browser, que contiene un servicio *Virtual Private Networks*[181] (VPN) gratuito como *CyberGhost o F-Secure Freedome* y un bloqueador de anuncios (*ad-blocker*) compatibles con Android. Dado que estas redes virtuales podrían no cambiar el número de serie del disco rígido, los expertos de ISIS recomendaron a sus seguidores utilizar un software gratuito denominado *Hard Disk Serial Number Changer.*

Para proteger los mails, los miembros del Estado Islámico emplean sistemas de encriptamiento gratuitos, la mayoría de los cuales han sido desarrollados en occidente, como Hushmail (proporciona una funcionalidad de verificación de dos pasos y alias ilimitados de correo electrónico), *Protonmail* (ofrece cifrado punta a punta, una cuenta de correo electrónico anónima y la seguridad inherente a las estrictas leyes de privacidad suizas), *Tutanota* (que no solo encripta el contenido, sino que también el objeto y los agregados) y/o *YOPmail* (que no requiere registro alguno o palabra clave).

Debido a que los teléfonos inteligentes les son de gran utilidad, pero a que no están exentos de ser localizados, comenzaron a utilizar *Telgram*, que ofrece el envío de mensajes cifrados desde el dispositivo emisor y descifrados, una sola vez, solo por el emisor y receptor que tengan la misma clave, y otras aplicaciones de seguridad como *Locker*, que elimina automáticamente los archivos del usuario cuando el número de intentos incorrectos de desbloqueo de la clave de pantalla incorrecto traspasa cierto umbral, o *FAKE GPS* que proporciona una falsa localización física cuando se utiliza en conjunto con ciertas plataformas de redes sociales.

En lo que respecta a los sistemas de encriptado, independientemente de la sofisticación de la plataforma, los yihadistas no confían totalmente en ningún servicio porque la mayoría se desarrolla en occidente. Para resolver este problema es que, en febrero de 2013, una unidad de logística de los medios de comunicación yihadista llamada *Global Islamic Media Front* (GIMF), introdujo *Asrar al-Dardashah* (secretos del chat), un *plug-in*[182] de cifrado compatible con plataformas de mensajería instantánea como Paltalk, Google Chat, Yahoo, MSN, y Pidgin.

---

180 Alkhouri, Laith & Kassirer, Alex, Tech for Jihad, July 2016; Disponible en: https://www.flashpoint-intel.com/wp-content/uploads/2016/08/TechForJihad.pdf

181 Una red privada virtual (RPV), en inglés: Virtual Private Network (VPN), es una tecnología de red de computadoras que permite una extensión segura de la red de área local (LAN) sobre una red pública o no controlada como Internet. Permite que la computadora en la red envíe y reciba datos sobre redes compartidas o públicas como si fuera una red privada con toda la funcionalidad, seguridad y políticas de gestión de una red privada. Esto se realiza estableciendo una conexión virtual punto a punto mediante el uso de conexiones dedicadas, cifrado o la combinación de ambos métodos. Ejemplos comunes son la posibilidad de conectar dos o más sucursales de una empresa utilizando como vínculo Internet, permitir a los miembros del equipo de soporte técnico la conexión desde su casa al centro de cómputo, o que un usuario pueda acceder a su equipo doméstico desde un sitio remoto, como por ejemplo un hotel. Todo ello utilizando la infraestructura de Internet.

182 Plug-in es un módulo de hardware o software que añade una característica o un servicio específico a un sistema más grande. La idea es que el nuevo componente se enchufa simplemente al sistema existente. Por ejemplo, hay un gran número de plug-ins para el navegador Firefox que permiten utilizar diversas herramientas y el plug-in de Flash, permite ver animaciones en Flash en cualquier navegador.

Por último, Alkhouri y Kassirer señalan que, si bien las herramientas mencionadas anteriormente permiten a los usuarios proteger sus actividades y evitar la detección, no garantizan la conectividad ininterrumpida a Internet, la cual resulta crucial para sus actividades. En los últimos años han desarrollado aplicaciones de propaganda móvil de su propiedad como *The A'maq Agency, Al-Bayan Radio, Voice of Jihad o Alphabet*.

Cabe agregar que no solo delincuentes y terroristas utilizan estas herramientas; las fuerzas armadas también las emplean para, por ejemplo:

- **Esconder puestos de comando y control:** cuando Internet fue diseñado por DARPA, su propósito principal era poder facilitar la comunicación distribuida, robusta en caso de huelgas locales. Sin embargo, algunas funciones deben ser centralizadas, como los sitios de comando y control. Es parte de la naturaleza de los protocolos de Internet el revelar la ubicación geográfica de cualquier servidor que es accesible en línea. La capacidad de los servicios ocultos de Tor permite a los puestos de comando y control militares estar físicamente seguros, no ser descubiertos y, de esa manera, reducir las posibilidades de ser atacados.
- **Proteger la vida de los militares:** no es difícil para los insurgentes supervisar el tráfico de Internet y descubrir todos los hoteles y otros lugares desde los cuales el personal militar se conecta a servidores militares conocidos. Los militares desplegados fuera de su casa usan Tor para ocultar los sitios que están visitando, resguardar sus intereses y operaciones militares, así como también para protegerse de daños físicos.
- **Recolección de inteligencia:** el personal militar necesita utilizar recursos electrónicos que ejecuta y controla el oponente, pero para ello deben evitar que este pueda registrar una dirección militar y quede al descubierto la operación de vigilancia que se está llevando a cabo.

Es por todo ello que, cuanto más se entienda sobre cómo se aprovechan las tecnologías digitales para participar en actividades adversas, mejor equipados se estará para defender y mitigar el riesgo tan eficazmente como sea posible.

La gobernanza de Internet

Cuando las cámaras de vigilancia aparecieron en la década de los 70 fueron recibidas como una herramienta de lucha contra la delincuencia, como una forma de monitoreo de la congestión del tráfico, de fábricas y hasta cunas de bebés. Más tarde, fueron adoptadas para propósitos más sombríos, como controlar a los manifestantes y disidentes.

Hoy en día, esas cámaras - y muchos otros dispositivos - conectados a Internet - han sido apropiadas para un propósito totalmente diferente: como una ciberarma de destrucción masiva. La desaceleración de Internet que se extendió por la costa este de los Estados Unidos e incluso de la Argentina con el sitio Infobae, el viernes 21 de octubre de 2016, ofrece una visión de una nueva era de las vulnerabilidades frente a una sociedad altamente conectada.

El ataque a la infraestructura de Internet, que hace casi imposible a veces comprobar los *feeds RSS* de Twitter[183] o los encabezados, es una muestra de cómo miles de millones de dispositivos ordinarios conectados a Internet - muchos de ellos altamente inseguros, pueden convertirse en propósitos perversos; y las amenazas continuarán para aquellos que cada vez más mantienen sus datos en la nube[184].

¿Qué sucedió? Un nuevo tipo de software malicioso se aprovechó de una vulnerabilidad largamente conocida de esas cámaras y otros dispositivos económicos que ahora se están uniendo a lo que se conoce como la Internet de las cosas, cuyos equipos son mucho más fáciles de comprometer, ya que ni las empresas los tienen en cuenta ni se actualizan a tiempo.

Como señalan Sanger y Perlroth[185]

> La ventaja de poner todos los dispositivos en Internet es evidente. Significa que la impresora de su casa pueda pedir a un vendedor que necesita más tinta, que las cámaras de seguridad puedan avisarle a su teléfono móvil que alguien está caminando por la entrada de su casa, ya sea un delivery o un ladrón. Cuando Google y los fabricantes de automóviles de Detroit instalen sus autos sin conductor en las calles y carreteras, la Internet de las cosas será su chofer.

Pero cientos de miles y quizás millones de esas cámaras de seguridad y otros dispositivos han sido infectados con un programa bastante sencillo que deducía o conjeturaba sus contraseñas de fábrica - a menudo *"admin"* o "12345" o incluso, *"password"* o "contraseña" - y una vez dentro, se convertía en un ejército de simples robots. Cada uno fue enviado, de manera coordinada, para bombardear una pequeña empresa en Manchester, New Hampshire, llamada Dyn DNS con mensajes que sobrecargaron sus circuitos. Dyn DNS actúa como un tablero gigante de Internet. Si se detiene, los problemas se difunden instantáneamente y no se necesita mucho tiempo para llevar a Twitter, Reddit, Airbnb y los feeds del *The New York Times* a un desastre.

Chester Wisniewski, investigador principal de computadoras en la firma Sophos, una empresa de seguridad, dijo que los asaltos como el de Dyn en lo que dio en llamar-

---

183 Un «Archivo RSS» o «Feed RSS» es un archivo generado por algunos sitios web (y por muchos weblogs) que contiene una versión específica de la información publicada en esa web. Cada elemento de información contenido dentro de un archivo RSS se llama "ítem". Cada ítem consta normalmente de un título, un resumen y un enlace o URL a la página web de origen o que contiene el texto completo. Además, puede contener información adicional como la fecha de publicación o el nombre del autor del texto.

184 La nube es un centro de almacenamiento de todos los datos que se almacenan en Internet, como, por ejemplo, las fotos de Facebook, correos electrónicos, registros médicos, información sobre impuestos, etc. Por razones de seguridad, muy pocas personas trabajan en ellos y el acceso es casi imposible, tanto así que incluso las personas que trabajan en los centros de datos no lo hacen en ellos, sino que, en sus hogares o en oficinas ubicadas en cualquier lugar del mundo. En otras palabras, lo que normalmente estaría almacenado en una PC (programas o archivos, por ejemplo) pasa a estar en los servidores que forman la nube. Por eso se habla en inglés de Cloud Computing, que suele abreviarse simplemente como The Cloud.

185 Sanger, David E. and Perlroth, Nicole. Era of Internet Attacks Powered by Everyday Devices; Disponible en: http://www.nytimes.com/2016/10/23/us/politics/a-new-era-of-Internet-attacks-powered-by-everyday-devices.html?rref=collection%2Fsectioncollection%2Fus&action=click&contentCollection=us&region=stream&module=stream_unit&version=latest&contentPlacement=7&pgtype=sectionfront&_r=122, 2016

se "*Internet Friday*", "podrían ser el comienzo de una nueva era de ataques de Internet a través de las cosas "inteligentes""[186].

Como señala Paul Rexton Kan[187],

> ...lo que está presente en varios grados en toda la literatura sobre el ciberespacio y la ciberguerra son los cinco debates distintos y constantes sobre este nuevo dominio y cómo actuar en el mismo. Los debates incluyen quién establece los límites del ciberespacio; cómo debe controlarse la información en línea; para quién debe estar disponible la información; determinar si pueden coexistir jerarquías y redes de personas en el ciberespacio; y establecer cuál es la diferencia entre "guerra" y "delito" en el ciberespacio.

Como era de esperar, todos estos avances tecnológicos requirieron que se establecieran algunas reglas sobre la gobernanza de Internet ya que lo que inicialmente era una ventaja, pronto se convirtió en una amenaza a la seguridad de las naciones. Nye y Donahue juzgan que por gobernanza se puede entender "la estructura y los procesos para una decisión colectiva, que involucra a actores gubernamentales y no-gubernamentales"[188]. Desde un enfoque institucional se aplica a las acciones, procesos y mecanismos de participación, por los cuales la autoridad es ejercida y las decisiones son tomadas e implementadas[189]. Otra definición es la que dice que por gobernanza se entiende el conjunto de mecanismos, acuerdos y estructuras por medio del cual un grupo social coordina su acción[190].

Por lo tanto, la gobernanza implica la intervención de aquellos sujetos o entidades que son decisivos, o que de algún modo están involucrados en un tema específico, siendo su participación a multinivel, y corresponde a los responsables de la administración, la formulación y ejecución de políticas[191]. En cuanto a la "gobernanza de riesgos", esta adapta los principios y los métodos del mecanismo básico de gobernanza en un entorno de riesgos, gestionando la complejidad y la incertidumbre[192] y en el ámbito institucional será la capacidad de las organizaciones y de los ciudadanos en general, para hacer frente

---

186 Ibidem.

187 Rexton Kan Paul; "Cómo analizar la guerra en Wi-Fi De ciberguerra a Wikiguerra: la lucha por el ciberespacio" Military Review septiembre-diciembre 2014; P. 30

188 Nye, J. and J. Donahue (edits.) (2000). Governance in a Globalizing World, Washington, D.C., Brookings Institution.

189 International Risk Governance Council [IRGC] (2006), White Paper on Managing and Reducing Social Vulnerabilities from Coupled Critical Infrastructures, Geneva.

190 Pisanti Baruch Alejandro, Gobernanza de Internet y los principios multistakeholder de la Cumbre Mundial de la Sociedad de la Información; Disponible en: http://portal.sre.gob.mx/imr/pdf/Pisanty.pdf

191 Masera G. y Ortiz J.U. (2015). Gobernanza de riesgos en la sociedad de la información en Conceptos y lenguajes, en ciencia y tecnología. Ed. Guillermo Cuadrado & Juan Redmond & Rodrigo López O. Valparaíso, Chile.

192 Aven, T. and O. Renn (2010). Risk Management and Governance. Concepts, Guidelines and Applications, Berlin, Springer Verlag.

a riesgos inevitables. Una "buena" gobernanza será la identificación, evaluación, gestión y comunicación de los riesgos[193].

A partir de la Cumbre del Milenio, la ONU identificó que, junto con graves problemas a los que dedicaría sendas cumbres, como el agua, la salud y la pobreza, la humanidad al llegar al tercer milenio de la era cristiana, había creado un área de oportunidad, el uso inteligente y apropiado de las TIC, para dar paso a una evolución global hacia la Sociedad de la Información, como una etapa positiva de la humanidad. En un intenso tironeo político, la UIT acabó imponiéndose a la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO), en contra de la opinión global de numerosos académicos y organizaciones de la sociedad civil, como organizador de la Cumbre Mundial sobre la Sociedad de la Información (CMSI o WSIS,)[194].

Quienes favorecían a la UNESCO como líder de la organización de la Cumbre, se basaban en la idea de que la Sociedad de la Información está definida ante todo por la información y el conocimiento; por su creación y propagación; por el acceso a ellos, y no por el despliegue de la infraestructura tecnológica de comunicaciones y el conocimiento técnico para operarla, que serían más propios del encargo de la UIT. Por otra parte, la ambición puntual de la UIT se concentraría en el control de la asignación de direcciones IP, interpretadas como parte de los planes fundamentales de las redes de telecomunicaciones, y en los nombres de dominio, toda vez que sobre éstos pueden emitirse reclamaciones en términos de soberanía nacional[195].

En abril de 2014, en San Pablo, se desarrolló la Reunión Global de Múltiples Partes Interesadas (*multishakeholder*) sobre el Futuro de la Gobernanza de Internet (NET mundial). Allí, representantes de alrededor de 80 países suscribieron a la Declaración Multisectorial la cual indica la necesidad de incrementar la cooperación y el diálogo sobre la gobernanza de Internet para fijar parámetros entre amenazas y derechos y que las iniciativas en ciberseguridad deben implicar la colaboración tanto de gobiernos como del sector privado, la sociedad civil, la academia y la comunidad tecnológica[196].

El documento plantea:

- Fundamentar estrategias para la inserción de América Latina en la comunidad internacional denominada SI;
- Planificar un sendero de crecimiento de las Tecnologías de Información y Comunicaciones, teniendo en cuenta riesgos y amenazas potenciales;
- Implementar mecanismos de participación para la gestión de riesgos, basados en el desarrollo sostenible y la gobernanza;

---

193 International Risk Governance Council [IRGC] (2010). Emerging risks. Sources, drivers and governance issues, Geneva, Revised edition.

194 Pisanti Baruch Alejandro, Gobernanza de Internet y los principios multistakeholder de la Cumbre Mundial de la Sociedad de la Información; Disponible en: http://portal.sre.gob.mx/imr/pdf/Pisanty.pdf P. 24.

195 Ibidem.

196 NETmundial (2014). "Multistakeholder Statement" (April, 24th, 2014); Disponible en: http://netmundial.br/es/about/

› En un plano más operativo, formular las bases para políticas públicas encaminadas a la gestión y regulación del riesgo.

En la Argentina, el 22 de abril de 2014 se creó la Comisión Argentina de Políticas de Internet (CAPI) dentro de la Secretaría de Comunicaciones[197]. Firmó la resolución el Secretario de Comunicaciones Norberto Berner que invita a una serie de organismos gubernamentales nacionales relacionados con la administración de Internet a sumarse a la Comisión, aunque no detalla plazos. El propósito es "diseñar una estrategia nacional sobre Internet y su gobernanza", que "tiene entre sus objetivos brindar soporte técnico y contribuir a una mayor y mejor representación de la República Argentina en los foros y organismos internacionales". Esta Resolución explica que, con respecto a la gobernanza de Internet, los puntos más relevantes para el crecimiento de los países son: garantizar la intimidad y la protección de datos personales de los ciudadanos, la seguridad nacional, la neutralidad en la red, la administración de sus recursos, el modelo multipartito de su gobernanza y los desafíos económicos y financieros y tributarios del uso extendido de Internet[198].

Surge entonces la pregunta ¿quién ejerce lo que se denomina gobernanza de Internet?

Gobernanza de Internet es establecer quién comanda su desarrollo, al menos el normativo. Estados Unidos anunció en 1998 la intención de transferir la custodia de las funciones de la Autoridad de Números Asignados (IANA) de ese país a la comunidad global de múltiples partes interesadas. IANA es una institución clave en la administración de Internet desde su inicio, pero es un organismo que nació como parte del gobierno estadounidense. Dicho de otra manera, el gobierno de Estados Unidos solicitó a la ICANN (*Internet Corporation for Assigned Names and Numbers*), una organización internacional sin fines de lucro responsable de signar direcciones IP, administrar dominios genéricos y territoriales para que lidere un proceso para que diferentes actores como la sociedad civil, el gobierno, y las empresas dialoguen en igualdad de condiciones. De esta manera, se busca evitar que un solo actor tome las responsabilidades de Internet[199].

Sin embargo, hay algunos que propugnan que sea la Organización de las Naciones Unidas quien lleve a cabo la gobernanza de Internet. Los que así piensan olvidan que en ONU se obedece a los más poderosos, que finalmente se impone la opinión de los gobiernos, y que la ONU no está preparada para gobernar Internet y regular las decisiones sobre políticas internacionales que darán forma al futuro de Internet.

Para los que propician una gobernanza abierta, se sostiene la opinión de que el hecho de que Internet sea gobernada por un esquema distribuido es una gran noticia

197 República Argentina. Ministerio de Planificación Federal, Inversión Pública y Servicios. Secretaria de Comunicaciones Disponible en: http://www.regulatel.org/wordpress/?portfolio=se-crea-comision-argentina-de-politicas-de-internet-capi

198 Diario La Nación: Crean una Comisión Nacional para la gobernanza de Internet. 23 de abril de 2014 Disponible en: http://www.lanacion.com.ar/1684422-Crean-una-Comisión-nacional-para-la-gobernanza-de-Internet

199 Internet se considera un derecho básico y la Cámara de Representantes de EEUU aprobó a principios del 2015 un proyecto de ley para evitar que puedan aplicarse impuestos a Internet y servicios on-line.

porque tiene que ver con la esencia de Internet. Se ve aquí una lucha por el poder, ya que Rusia y China critican el modelo de gestión propuesto por Estados Unidos basado en los *multishakeholders*, y lo que se pretende en realidad es controlar estrictamente a Internet. Rusia y China proponen un modelo consensuado.

Internet se considera un derecho básico y la Cámara de Representantes de Estados Unidos aprobó a principios del 2015 un proyecto de ley para evitar que puedan aplicarse impuestos a Internet y servicios on-line.

El gobierno argentino que finalizó en el año 2015 parecía estar tomando la dirección opuesta, ya que pretendía controlar los comentarios de medios digitales y plataformas de Internet con la excusa de la ley de antidiscriminación. Sin embargo, si un argentino en el exterior publicara en *Facebook*, que es una empresa estadounidense, un comentario discriminatorio de otro argentino no estaría sujeto a las leyes argentinas.

Pero como en última instancia todo se trata de un equilibrio entre libertad y seguridad, ya hay posturas que objetan cualquier clase de control sobre Internet, como la Fundación Vida Libre, que sostiene que "existe el mito de que ICAAN solo se ocupa de cuestiones técnicas, cuando en realidad no hace prácticamente nada que pueda remotamente vincularse con cuestiones técnicas. La existencia de ICAAN ha transcurrido en la promoción de planes de ciertos selectos intereses comerciales (particularmente de Estados Unidos y Europa) y evitando involucrarse en cuestiones que atiendan la estabilidad técnica de Internet. Se dice que ICAAN administra, coordina y asigna direcciones IP: falso. Se dice que ICAAN administra y coordina el sistema de servidores raíz; falso también. Algunos sostienen que la tarea de promover la competencia en el espacio de dominios genéricos de nivel superior (gTLD) es una tarea técnica. Eso es una broma de mal gusto. Por último, ICAAN ha creado una política global de resolución de disputas sobre nombres de dominio que no tiene ningún componente técnico y es un acto regulatorio supranacional basado en la coerción[200].

En el texto de la resolución 13 de la Secretaría de Comunicaciones[201] se indica que "El concepto de "Gobernanza de Internet" fue definido como "el desarrollo y aplicación por los gobiernos, el sector privado y la sociedad civil de las funciones que les competen respecto de principios, normas, reglas, procedimientos de adopción de decisiones y programas comunes que configuran la evolución y la utilización de Internet". Esto surge de la Cumbre Mundial de la Sociedad de la Información celebrada en TÚNEZ en el año 2005"[202].

Antes bien parece una solución de compromiso tendiente a controlar las opiniones en Internet.

---

200 El gobierno de Internet, artículo aparecido el 6 de agosto de 2004, página 1; Disponible en: http://www.vialibre.org.ar/2004/08/27/el-gobierno.de-la-Internet

201 República Argentina. Ministerio de Planificación Federal, Op. Cit.

202 Compromiso de Túnez; Disponible en: http://www.itu.int/net/wsis/docs2/tunis/off/7-es.html

Conclusiones del capítulo

La llegada y evolución del espacio cibernético ha transformando el mundo y revolucionado la vida diaria de los habitantes del globo. Al igual que en el mar, la tierra o el aire, el espacio cibernético es un dominio en el que los seres humanos maniobran en y a través de él para lograr objetivos en los espacios físicos donde viven. No tiene fronteras geográficas, la tecnología es barata y se encuentra al alcance de cualquiera, la autoría de acciones perniciosas es anónima, y sus autores oscilan desde adolescentes hasta organizaciones criminales, algunas independientes y otras, que aparecen como tales, son apoyadas por algunos gobiernos.

Una de las tantas cosas que ha cambiado en esta era es la velocidad a la que se mueve la información alrededor del mundo, su profundidad de penetración en la sociedad y la continua invención y adaptación de medios electrónicos y software para uso humano y automatizado.

A través del espacio cibernético, la información se traslada por medio de contenidos y códigos (software) y lo que puede ser visto como el entrelazamiento del espacio cibernético y la actividad humana, el número de seres humanos utilizando el espacio cibernético para las actividades comunes (comunicación, navegación, noticias, compras, banca, entretenimiento, etc.) aumenta rápidamente. Esta rápida evolución de la red, junto con su poder de conexión, ha generado grandes oportunidades económicas y sociales imprevisibles hace veinte años atrás.

La dependencia del espacio cibernético diluye las fronteras geográficas, derriba las divisiones culturales y religiosas tradicionales, une a las familias y a los amigos y permite el contacto entre aquellos que comparten intereses o preocupaciones. Ha cambiado la forma de comunicarse.

En cuanto a si el espacio cibernético es transversal a todos los ámbitos convencionales, o si es independiente de los ámbitos convencionales, puede decirse que cada fuerza terrestre, marítima y aérea tiene aspectos cibernéticos específicos, en especial los correspondientes a los sistemas de armas en su relación sensor –disparo, además de los propios de las estructuras de comando y control específicas en cada ámbito geográfico de competencia.

En este sentido, ocurre lo mismo que aconteció con la Fuerza Aérea. En un principio, existía la aviación en el Ejército y en la Armada, hasta que se conformó la Fuerza Aérea como ámbito independiente. No obstante, las fuerzas terrestres y navales continuaron manteniendo elementos aéreos necesarios en apoyo directo para cumplir las misiones de su ambiente específico. El poder aéreo no cambió la naturaleza de la guerra, pero sí su carácter y la forma en que fue conducida.

Sin embargo, aunque inicialmente existió la opinión de que dado lo incipiente de su desarrollo, todavía las acciones en el espacio cibernético deben considerarse únicamente un sistema de armas, en el concepto mundial se considera ya un ámbito específico de actuación.

Muchos países así lo entendieron y crearon cibercomandos u oficinas dedicadas en particular a la defensa cibernética. Para ser precisos, el concepto de ciberguerra comprende tanto las acciones defensivas como las ofensivas que tienen lugar en ese ciberespacio, compuesto por todas las dimensiones que se detallaron.

Esta dificultad en definir el término espacio cibernético genera, entre otras cosas, conflictos cuando se pretende alcanzar cualquier tipo de acuerdo común entre los estados en cuanto a cómo debe aplicarse el Derecho Internacional de los Conflictos Armados porque en él se pueden ejecutar, de manera independiente de los otros, operaciones de información.

No obstante, y a pesar de la imposibilidad de obtener una clara definición respecto de qué es el espacio cibernético, hoy en día resulta casi imposible pretender emplear plenamente una fuerza conjunta sin aprovecharlo.

En el espacio cibernético no es necesario ningún pasaporte. Aunque las policías están limitadas por las fronteras nacionales, los criminales deambulan libremente. Los enemigos ya no están al otro lado del océano, sino apenas detrás de un *firewall*. El malintencionado puede enmascarar su identidad y su ubicación, suplantar la identidad de otros y estudiar detenidamente su camino hacia los edificios que mantienen la riqueza digitalizada de la era electrónica: dinero, datos personales y propiedad intelectual.

En lo que respecta a la definición de guerra cibernética, si se considerase procedente utilizar dicho término, se recomienda adoptar la del Consejo de Seguridad de las Naciones Unidas según la cual "guerra cibernética significa el uso de computadoras o medios digitales por un gobierno o con el conocimiento explícito o la aprobación de ese gobierno contra otro estado, o propiedad privada dentro de otro estado, lo que incluye: el acceso intencional, interceptación de datos o daños a la infraestructura digital y a la infraestructura controlada digitalmente y la producción y distribución de dispositivos que pueden usarse para subvertir la actividad interna".

Sin embargo, es necesario tener presente que hoy en día, las confrontaciones y conflictos que tienen lugar en el espacio cibernético pueden no ocurrir necesariamente en el contexto de una guerra, ni siquiera en el de una confrontación general. De aquí que el término guerra cibernética, como fuera dicho, es algo más descriptivo y representa la lucha entre dos estados o facciones de los mismos, o actores no estatales que tiene lugar en el espacio cibernético.

Tampoco existe un acuerdo internacional respecto de cuáles deben ser consideradas como operaciones cibernéticas que afectan a la Defensa Nacional. Podría decirse que, de los casos estudiados, consistirían en aquellas que dañen las infraestructuras críticas de la Defensa Nacional y, dentro de un Teatro de Operaciones, aquellas que pudieran perjudicar el ejercicio del comando y control y la libertad de acción en el espacio cibernético[203].

Tampoco existe un acuerdo internacional respecto de cuáles deben ser consideradas como operaciones cibernéticas que afectan a la Defensa Nacional. Podría decirse que, de los casos estudiados, consistirían en aquellas que dañen las infraestructuras críticas de la Defensa Nacional y, dentro de un Teatro de Operaciones, aquellas que

203 Si bien no han sido objeto de esta investigación, no se puede negar la existencia de las operaciones ofensivas destinadas a producir una variedad de efectos fuera de las propias redes militares, para satisfacer las necesidades de la seguridad nacional.

pudieran perjudicar el ejercicio del comando y control y la libertad de acción en el espacio cibernético[204].

En los documentos analizados, se consideran ciberoperaciones todas aquellas operaciones ejecutadas para interrumpir, negar, degradar o destruir la información existente en las computadoras y redes de computadoras, o las computadoras y redes propiamente dichas. Pueden ser una forma avanzada del uso de la fuerza que precede al esfuerzo principal en el Teatro de Operaciones a fin de preparar al objetivo para el asalto principal. Pueden incluir el reconocimiento (mapeo de una red), la captura de posiciones de apoyo (el asegurar el acceso a nodos o a sistemas clave de redes) y el pre posicionamiento de armas o capacidades (implante de herramientas de acceso cibernético o códigos maliciosos). Además, pueden ser un método para obtener inteligencia extranjera ajena a objetivos militares específicos, como la comprensión de desarrollos tecnológicos u obtener información sobre las capacidades militares y la intención del adversario.

Más allá de las pequeñas diferencias existentes entre las doctrinas de los Estados Unidos y las de la Organización del Tratado del Atlántico Norte (OTAN), la Unión Europea y Brasil, que adhiere al criterio europeo, puede decirse que las operaciones cibernéticas son ofensivas, defensivas – activas y pasivas – y de exploración, las cuales incluyen las operaciones de ciber inteligencia, de vigilancia y reconocimiento (IVR) y las operaciones cibernéticas de preparación del ambiente operacional.

En lo concerniente a las agresiones cibernéticas, se concluye que para que un ciberataque pueda ser calificado como un "ataque armado" por el Derecho Internacional de los Conflictos Armados, debería lograr que algo físico deje de funcionar o funcione incorrectamente. Por tal motivo, no se incluyen o no deberían incluirse las procedentes de individuos u organizaciones con fines de extorsión, estafa o chantaje a ciudadanos u organizaciones privadas.

Muchos usos coloquiales de la palabra "ataque" en referencia a algún tipo de incidente cibernético, ya sea público o privado, (fraudes, amenazas, sabotaje, robo de información, phishing masivos, ataques de DOS) no son necesariamente "ataques armados" a los efectos de ejercer el derecho inherente de un Estado a auto defenderse bajo el *jus ad bellum*, y, de hecho, no son necesariamente ataques a los fines de la aplicación de las normas para llevar a cabo ataques durante la conducción de las hostilidades.

Independientemente de cuál sea la definición que se adopte, debe quedar claro que en lo que respecta a la Defensa Nacional, los ataques cibernéticos presentan una nueva y creciente amenaza, que el derecho internacional y la mayoría de las leyes nacionales actuales no están en condiciones de enfrentar. El Derecho Internacional de los Conflictos Armados, citado a menudo como el plexo legal competente, de hecho, solo es una base para responder a los ataques cibernéticos que sean equivalentes a un ataque armado. Otros documentos internacionales existentes, como el "Manual de Tallin 2.0 sobre el Derecho Internacional aplicable a las operaciones cibernéticas", solo ofrecen una protección embrionaria o fragmentada.

---

204 Si bien no han sido objeto de esta investigación, no se puede negar la existencia de las operaciones ofensivas destinadas a producir una variedad de efectos fuera de las propias redes militares, para satisfacer las necesidades de la seguridad nacional.

Desde el punto de vista militar, las capacidades a desarrollarse deberían permitir ejercer el mando y control, es decir, dirigir y coordinar las fuerzas en operaciones. Dado que muchos de estos sistemas de mando y control dependen del espacio cibernético para funcionar, y que para ello requieren de una infraestructura TIC para transmitir la información, deberán ser seguros y resilientes[205] frente a los ciberataques y tendrán que estar permanentemente operativos para poder dirigir las operaciones.

Estas capacidades deberían poseer, además, la aptitud o suficiencia para poder retener la libertad de acción en el espacio cibernético y prevenir sorpresas estratégicas en esa dimensión, dentro de un determinado tiempo y por un plazo establecido. Por ello, será necesario disponer tanto de cibercapacidades - defensivas y de inteligencia - como de expertos en TICs.

Dado que la actitud ofensiva está prohibida en la ley internacional, todos dicen defenderse frente a estos ataques, aunque otros, como la OTAN, ya utilizan el término de "defensa activa" según se lancen o no contraataques sobre los agresores. Tanto es así, que hasta ya existen Reglas de Empeñamiento cibernéticas. La Argentina, por imperio de la separación entre seguridad interna y defensa externa, y con la prohibición absoluta de cualquier acción ofensiva, ha optado por hablar de "defensa directa" y "defensa indirecta", circunloquios que impiden a otros países del mundo entender sus significados.

Quienes continúan hablando solamente de acciones defensivas olvidan la íntima conexión entre ataque y defensa, ya que el apotegma de Clausewitz sigue vigente: "una defensa no es sino un escudo hecho con golpes bien dirigidos"[206]. Restringir a la defensa informática entendiéndola únicamente como seguridad cibernética es perder toda iniciativa y libertad de acción en este nuevo ambiente.

Si se entiende a la ciberseguridad, en cambio, como un objetivo y a la ciberdefensa como un medio para alcanzarla, la ciberdefensa en las fuerzas armadas debe, como fuera dicho, garantizar la libertad de acción de las operaciones militares en el espacio cibernético y apoyar la respuesta coordinada entre los diferentes actores, tanto nacionales como internacionales, ante un ciberataque que pueda afectar a la Defensa Nacional.

La agresión cibernética se debe enfrentar por su naturaleza y no por su lugar de origen, por lo que diferenciar seguridad interna de ataque militar externo es un ejercicio ocioso e inútil del criterio. La disparidad de conceptos de seguridad y defensa en los países de UNASUR, la diferencia de significados relativos a este nuevo ámbito, y el uso de medios asimétricos para hacerle frente impide cualquier cooperación regional por más que sea declamada en frondosos documentos diplomáticos.

Por último, debe quedar claro que ciberespacio e Internet no son sinónimos, Internet es un subconjunto más pequeño del ciberespacio más grande.

---

205 Al igual que un cuerpo humano que puede sufrir a causa de los virus pero que gracias a ellos se vuelve más fuerte y resistente, las nuevas tecnologías, soluciones y esfuerzos colaborativos hacen que Internet sea más resiliente ante las actividades maliciosas.

206 Clausewitz, Carl, On War, Indexed Edition, Edited and Translated by Michael Howard, and Peter Paret, Princeton University Press, New Jersey, Año 1989, Book 6 Chapter 1 P. 357

La forma en que se gobierna Internet ha sido siempre un tema muy debatido. Se ha podido comprobar que Internet es un fenómeno complejo con una larga tradición de autorregulación, concepto con el cual muchas empresas y gobiernos están muy apegados.

La naturaleza descentralizada de Internet significa que no hay ninguna autoridad única y centralizada a cargo de su gestión, lo cual garantiza que los problemas puedan resolverse en el nivel más cercano a su origen. Sin embargo, hay otros que consideran que deben intervenir más en su gestión y su coordinación internacional, pues opinan que Internet es tan importante que debe considerarse como una cuestión de interés nacional y, por lo tanto, se sienten obligados a intervenir.

CAPÍTULO 2

ESTRATEGIAS O POLÍTICAS NACIONALES EN EL CAMPO DE LA CIBERDEFENSA Y LA CIBERSEGURIDAD

Introducción

El concepto imperante en la Argentina según el cual la **seguridad** se refiere a la **seguridad pública interna** y la *defensa* a la **seguridad pública externa** no es universal y ni siquiera aceptada por entero en el ámbito regional. En principio, no existe consenso en el hemisferio occidental sobre las definiciones de seguridad y defensa; no obstante, en América Latina y el Caribe, la seguridad parece encapsular o abarcar todo excepto a las Fuerzas Armadas y eso es una consecuencia de la dificultad de armonizar las relaciones cívico-militares producto de las guerras civiles internas ocurridas en la década del 70 del siglo XX.

De resultas de esta situación arriba mencionada, en ciertas naciones de América Latina, especialmente en la Argentina rige, podría decirse metafóricamente, un "exorcismo intelectual" que consiste en establecer un "muro impermeable" entre seguridad y defensa, no solo como construcción intelectual sino como estructura operacional. Como consecuencia de ello, se considera entonces que la *seguridad* en tanto **seguridad pública interna** es de responsabilidad de las Fuerzas de Seguridad y Policiales; y *defensa*, en tanto **seguridad pública externa** es responsabilidad de las Fuerzas Militares. Otra consecuencia ha sido la proliferación de varios conceptos nuevos creados para calificar la seguridad tales como "seguridad democrática"[207], "seguridad ciudadana"[208], "seguridad ambiental", "seguridad multidimensional". Estos nuevos conceptos ciertamente

207 Seguridad democrática tiene diferentes significados según la región de que se trate. Para Colombia, significa una vida social libre de los peligros de grupos armados ilegales; para Centroamérica, significa una vida social donde se respeten los derechos individuales de las personas.

han contribuido a diluir las viejas nociones asociadas a la "seguridad nacional", pero también ayudaron a disolver el concepto mismo de "seguridad" y otros conceptos asociados directamente a esta[209].

En la República Argentina, el ex jefe de Gabinete del Ministerio de Defensa, Sergio Rossi, explicó en una entrevista con Télam[210] que:

> ...en nuestro país la política de seguridad de la información, protección de infraestructuras críticas y estándares tecnológicos vinculados a la cuestión cibernética es competencia de la Jefatura de Gabinete de Ministros, que desde hace más de una década dicta las recomendaciones y manuales de procedimiento
>
> Nuestra Ley de Defensa y su decreto reglamentario establecen que la misión de las Fuerzas Armadas es conjurar y repeler una agresión militar estatal externa. Identificar el origen y definir sus límites y alcances que, cuando hablamos del espacio cibernético exige un esfuerzo de construcción doctrinaria, capacidades tecnológicas y formación de recursos humanos, sostuvo.
>
> Algunas de esas infraestructuras pertenecen al ámbito de la defensa, y esas son las que merecen nuestra atención, porque son aquellas en que se apoya o resultan vitales para el instrumento militar. Por otra parte, hay una dimensión del problema que hace a amenazas vinculadas a los derechos de las personas y de índole individual, cuya naturaleza es criminal y competencia, por tanto, de las agencias de seguridad del Estado", agregó.

Aplicar este concepto pareciera contrariar los conceptos vigentes en el mundo luego de la Guerra Fría. Para Estados Unidos, Canadá, Europa y la OTAN, los términos de seguridad y defensa son intercambiables, y la eventual discusión sobre el rol de las Fuerzas Armadas dentro del contexto de seguridad no es problemático como todavía sigue siendo en algunos países de Centro y Sudamérica, donde "...la aceptación política de estos nuevos conceptos y vocablos de seguridad ha pasado a ser más importante que ocuparse de los problemas que verdaderamente afectan la seguridad a niveles ciudadanos, sociales, o del estado mismo en un ambiente político democrático"[211].

---

208 Para la Comisión Interamericana de Derechos Humanos, la expresión seguridad ciudadana surgió, fundamentalmente, como un concepto en América Latina en el curso de las transiciones a la democracia, como medio para diferenciar la naturaleza de la seguridad en democracia frente a la seguridad en los regímenes autoritarios. En estos últimos, el concepto de seguridad está asociado a los conceptos de "seguridad nacional", "seguridad interior" o "seguridad pública", los que se utilizan en referencia específica a la seguridad del Estado. En los regímenes democráticos, el concepto de seguridad frente a la amenaza de situaciones delictivas o violentas, se asocia a la "seguridad ciudadana" y se utiliza en referencia a la seguridad primordial de las personas y grupos sociales; Disponible en: https://www.cidh.org/countryrep/Seguridad/seguridadii.sp.htm

209 Woodrow, Wilson International Center for Scholars, Reforma de las FFAA en América Latina y el impacto de las amenazas irregulares, Editor José Raúl Perales, Washington DC, agosto de 2008, Comentario al Panel 3 Luis Bitencourt, P. 143 y 144.

210 Télam. Ciberdefensa: Argentina avanza en la construcción de elementos para su fortalecimiento. Sociedad. 28 de agosto de 2015; Disponible en: http://www.telam.com.ar/notas/201508/117946-ciberdefensa-argentina-avanza-en-la-construccion-de-elementos-para-su-fortalecimiento.html

211 The Woodrow Wilson International Center for Scholars, Latin American Program; Reforma de las FFAA en América Latina y el impacto de las amenazas irregulares. Bitencourt, Luis; Comentarios Panel 3; P. 145; Disponible en: http://www.cpalsocial.org/documentos/110.pdf

Esta contradicción ya había sido advertida por Brasil. Al hablar en la Conferencia de Ejércitos Americanos llevada a cabo en Brasilia en noviembre de 2007, el Ministro de Defensa de Brasil Nelson Jobim expresó:

> La defensa fue inicialmente percibida como algo asociado a la represión política; la seguridad pública fue asociada como enlazada a la represión política. Y tal identificación, de una forma u otra – nosotros no juzgamos valores, sino que solamente reconocemos la existencia de tal identificación, si entre asuntos de defensa y seguridad asociados con la represión política realmente existe - terminó distanciando al Ejército, a la Armada y a la Fuerza Aérea del diseño de las políticas nacionales. De esa forma, los asuntos militares fueron restringidos exclusivamente a la esfera militar. La nueva visión del gobierno de Brasil – una decisión hecha por el Presidente Lula – es incluir los asuntos de defensa en la agenda nacional, en vez de guardarla exclusivamente como un asunto militar. En otras palabras, integrar los asuntos de seguridad y defensa dentro de la perspectiva nacional de la corporación militar... [212]

En el tema que nos ocupa, esta división conceptual que asocia seguridad como interna, y defensa como externa no es aplicable a los problemas cibernéticos, principalmente porque, como fuera explicado, el espacio cibernético no tiene fronteras y en ciertos casos se podría distinguir entre delitos contra la seguridad pública y delitos contra la seguridad del estado, en la implementación las superposiciones son muy frecuentes.

Para tomar un ejemplo, en Alemania, en términos de ciberdefensa militar, el Departamento de Información y Operaciones de Redes de Computadoras (*Department of Information and Computer Network Operations*) de las fuerzas armadas tiene la tarea de desarrollar las capacidades cibernéticas. En cuanto a la ciberseguridad, el país publicó su estrategia en 2011 bajo la supervisión del Ministerio del Interior, que también estableció un Centro Nacional de Respuesta Cibernética (a *National Cyber Response Center*) en aquel momento. El centro incorporó a funcionarios de la Oficina Federal de Policía Criminal, la Policía Federal, la oficina criminológica de la aduana, el Servicio de Inteligencia Federal, los administradores de las infraestructuras críticas y obviamente a las fuerzas armadas. "También existe un Consejo Nacional de Ciberseguridad que se ocupa de la prevención de grandes ataques[213] y sus contramedidas, que incluye todos los ministerios y determinados actores privados y que, además, es responsable de coordinar las técnicas de defensa y la política cibernética"[214].

---

212 Conferencia de Ejércitos Americanos, Brasilia. Brasil, 2007: Palabras de apertura del Ministro de Defensa Nelson Jobim.

213 Ataques importantes: aquellos que las medidas de seguridad tradicionales (AV, firewall, IDS, DLP, etc.) no son capaces de dar respuesta de forma efectiva.

214 Gramaglia, Matteo, Tuohy, Emmet, Pernik, Piret; Military Cyber Defense Structures of NATO Members: An Overview; Disponible en: https://www.icds.ee/fileadmin/media/icds.ee/failid/Military%20Cyber%20Defense%20Structures%20of%20NATO%20Members%20-%20An%20Overview.pdf

En suma, los conceptos imperantes en el mundo que permiten comprender los riesgos y peligros de las amenazas cibernéticas son los de **seguridad**, que significa libre de riesgos y peligros que amenacen la existencia, y los de **defensa** que, en el caso de existir tales riesgos y amenazas a la seguridad, se encuentre en condiciones razonables de enfrentarlos con posibilidades de éxito. Los desafíos cibernéticos se encuentran dentro de las estrategias de seguridad nacional de los estados.

Para demostrarlo, a continuación, se presentan los análisis realizados sobre las estrategias nacionales en el campo de la ciberdefensa y de la ciberseguridad de algunos países de Europa y Sudamérica que se tomaron como estrategias referentes en estas áreas.

Las Estrategias o Política Nacionales de Ciberseguridad

Con posterioridad a los sucesos de Estonia en 2007, gobiernos de casi todo el mundo comenzaron a desarrollar políticas y estrategias en materia de seguridad de la información y de competencia en materia militar, así como también a crear organismos que centralizaran responsabilidades, realizaran diagnósticos y desarrollasen capacidades, tendientes a ser activos en materia de operaciones cibernéticas de seguridad, defensa y acción preventiva frente a agresiones en el espacio cibernético contra sus servicios e infraestructuras críticas.

Dichas políticas y estrategias, dejando de lado la clásica división referida al orden público entre seguridad interior y exterior del estado, adoptaron un concepto más amplio como es el de Seguridad Nacional, entendida hoy como el **estado deseado** por una sociedad en el que pueda esta desarrollarse y prosperar libre de amenazas[215].

En el documento UN Res AG 40/553 *Conceptos of Security* de 1986, la Asamblea General definió a la seguridad como "una condición por la cual los estados consideran que no existe peligro de una agresión militar, presiones políticas o coerción económica, de manera que pueden dedicarse libremente a su propio desarrollo y progreso"[216].

Actualmente, países como Brasil[217], Chile[218], España[219], Francia[220] y Perú[221] han adoptado un criterio similar en cuanto a que el estado es el responsable de la Seguridad Na-

---

215 Debe entenderse por **amenaza** a la percepción de la capacidad que un potencial adversario posee para infligir un daño o perjuicio, especialmente si no se actúa como él desea. Por otra parte, al **riesgo** se lo define como el grado de estimación o probabilidad de que una amenaza se materialice a través de vulnerabilidades propias, sobre uno o más activos propios causando daños o perjuicios en los mismos.

216 Documento AG 40/553 Conceptos of Security, Página 2. Punto 3; Disponible en: https://unoda-web.s3-accelerate.amazonaws.com/wp-content/uploads/assets/HomePage/ODAPublications/DisarmamentStudySeries/PDF/SS-14.pdf.

217 Brasil, Política Nacional de Defensa; Disponible en: http://www.defesa.gov.br/arquivos/2012/mes07/pnd.pdf

218 República de Chile, Libro de la Defensa Nacional de Chile 2010, Tercera Parte: Política de Defensa Nacional, Capítulo IX. Defensa y Seguridad, P. 128.

219 Estrategia de Seguridad Nacional 2013 del Reino de España; Disponible en: http://www.lamoncloa.gob.es/documents/seguridad_1406connavegacionfinalaccesiblebpdf.pdf

220 Francia, "Libro Blanco sobre Defensa y Seguridad Nacional"; Disponible en: http://www.livreblancdefenseetsecurite.gouv.fr/pdf/the_white_paper_defence_2013.pdf .

221 Perú, Libro Blanco de la Defensa del Perú, Capítulo III "Política de Estado para la Seguridad y la Defensa Nacional" P. 62 Disponible en: http://www.defesa.gov.br/projetosweb/livrobranco/arquivos/pdf/peru-libro-blanco-de-la-defensa-nacional2005.pdf.

cional y para alcanzarla disponen de una serie de medios e instituciones muy variados que van desde la justicia, la diplomacia o la política económica, hasta los que suponen el uso de la fuerza en sus distintas formas. Estos últimos son los que se engloban tradicionalmente en el concepto de Defensa, la que, "en un sentido genérico, involucra todas las previsiones y acciones tendientes a proteger y preservar los propios intereses de efectivas y potenciales amenazas"[222].

Un ejemplo de ello lo constituye Francia que, en 2008, en el prólogo del Libro Blanco de la Defensa y Seguridad Nacional, el entonces presidente Nicolás Sarkozy señalaba que "...la globalización ha cambiado profundamente tanto la vida económica como la vida cotidiana y las relaciones internacionales. Han surgido nuevos poderes y se revelan nuevas vulnerabilidades. La división tradicional entre seguridad interna y externa ha quedado eliminada"[223].

Un caso más reciente es el del Reino de España, cuya Ley de Seguridad Nacional,[224] aprobada en septiembre de 2015, establece que:

> La Seguridad Nacional se entiende como la acción del Estado dirigida a proteger la libertad y el bienestar de sus ciudadanos, a garantizar la defensa de España y sus principios y valores constitucionales, así como a contribuir junto a nuestros socios y aliados a la seguridad internacional en cumplimiento de los compromisos asumidos; concepto que, hasta la fecha, no había sido objeto de una regulación normativa integral.

En la exposición de motivos, se indica que:

> ...la realidad demuestra que los desafíos para la Seguridad Nacional que afectan a la sociedad revisten en ocasiones una elevada complejidad, que desborda las fronteras de categorías tradicionales como la defensa, la seguridad pública, la acción exterior y la inteligencia, así como de otras más recientemente incorporadas a la preocupación por la seguridad, como el medio ambiente, la energía, los transportes, el espacio cibernético y la estabilidad económica.
>
> A los efectos de la ley, se consideran componentes fundamentales de la Seguridad Nacional, la Defensa Nacional, la Seguridad Pública y la Acción Exterior, que se regulan por su normativa específica. Los Servicios de Inteligencia e Información del Estado, de acuerdo con el ámbito de sus competencias, apoyarán permanentemente al Sistema de Seguridad Nacional, proporcionando elementos de juicio, información, análisis, estudios y propuestas necesarios

222 República Argentina, PC 00-02, Glosario de Términos de Empleo Militar para la Acción Militar Conjunta, Proyecto 2015, P. 68.

223 Francia, "Libro Blanco sobre Defensa y Seguridad Nacional" Op. Cit. 215

224 España, Ley 36/2015, de 28 de septiembre, de Seguridad Nacional; Disponible en: http://noticias.juridicas.com/actualidad/noticias/10529-contenido-de-la-ley-36-2015-de-28-de-septiembre-de-seguridad-nacional/

para prevenir y detectar los riesgos y amenazas[225] y contribuir a su neutralización[226].

Lo que puede apreciarse de acuerdo al contenido de la legislación de Francia y de España es que dichos estados, al igual que otros, en la búsqueda de lograr un interés superior, procuran mejorar la coordinación de las diferentes administraciones públicas, buscando marcos de prevención y respuesta que ayuden a resolver los problemas que plantea una actuación compartimentada, organizando a diversos niveles y de manera integral la acción coordinada de los agentes e instrumentos al servicio de la Seguridad Nacional.

Para lograr el grado de coordinación necesario, como se verá en los casos de estudio que se desarrollarán a continuación, los países elaboran una serie de documentos derivados de las leyes de Seguridad Nacional y de Defensa Nacional, como por ejemplo las estrategias de Seguridad Cibernética, y las Estrategias de Ciberdefensa, mediante las cuales se establecen ámbitos prioritarios de actuación y se definen para cada uno de ellos, el objetivo principal a alcanzar y varias líneas de acción estratégicas, que enmarcarán las respuestas y actuaciones concretas que requiere la preservación de la seguridad nacional.

En una conferencia dada en la Escuela Superior de Ingenieros de Telecomunicaciones, Luis Feliú recomendó[227]:

> La Estrategia de Seguridad Nacional debe definir la forma de proteger el territorio, las infraestructuras críticas y a los propios ciudadanos. Todos los países en mayor o menor medida han desarrollado sus nuevas estrategias de Seguridad Nacional de acuerdo con las nuevas amenazas y consecuentemente establecido sus planes de Defensa tanto a nivel civil como militar. En ellas ocupa un lugar importante la ciberdefensa que comprende pues todas las acciones y medidas necesarias para garantizar la

---

225 Para España, son considerados riesgos y amenazas para la Seguridad Nacional, los conflictos armados, el terrorismo, las ciberamenazas, el crimen organizado, la inestabilidad económica y financiera, la vulnerabilidad energética, la proliferación de armas de destrucción masiva, los flujos migratorios irregulares, el espionaje, las emergencias y catástrofes, la vulnerabilidad del espacio marítimo y la vulnerabilidad de las infraestructuras críticas y servicios esenciales. También se contemplan los factores potenciadores como el cambio climático, la pobreza, la desigualdad, los extremismos ideológicos, los desequilibrios demográficos o la generalización del uso nocivo de las nuevas tecnologías, que, sin ser en sí mismos un riesgo o una amenaza, pueden desencadenarlos o agravarlos".

226 Según el proyecto, "La composición del Consejo de Seguridad Nacional se determinará conforme a lo previsto en el apartado 8 de este artículo. En todo caso, deberán formar parte de dicho Consejo:
a) El Presidente del Gobierno, que lo presidirá.
b) Los vicepresidentes del gobierno, si los hubiere.
c) Los Ministros de Asuntos Exteriores y de Cooperación, de Defensa, de Hacienda y Administraciones Públicas, del Interior, de Fomento, de Industria, Energía y Turismo, de Economía y Competitividad y de Sanidad, Servicios Sociales e Igualdad.
d) El director del Gabinete de la Presidencia del Gobierno, el Secretario de Estado de Asuntos Exteriores, el Jefe de Estado Mayor de la Defensa, el Secretario de Estado de Seguridad y el Secretario de Estado Director del Centro Nacional de Inteligencia.

227 Feliú, Luis, Seguridad Nacional y Ciberdefensa: Aproximación Conceptual: Ciberseguridad y Ciberdefensa, Conferencia en la Escuela Superior de Ingenieros de Telecomunicaciones, Madrid, 21 de enero de 2013; Disponible en: http://catedraisdefe.etsit.upm.es/wp-content/uploads/2013/01/Ponencia-Luis-Feliu.pdf

ciberseguridad es decir la seguridad de todos los CIS[228] tanto militares como civiles, públicos o privados.

Entre otras cosas, también señaló que la Unión Europea ya había establecido las normas para la protección de las infraestructuras críticas y el nivel de seguridad de los CIS y agregó que, en concreto, todos los países europeos coinciden en mayor o menor medida en que:

- Se deben definir claramente las amenazas y los riesgos existentes para la ciberseguridad y, como consecuencia de ellos, los objetivos a alcanzar, las medidas a tomar y las acciones a ejecutar. Allí se precisan los objetivos estratégicos a alcanzar, los órganos competentes y sus responsabilidades, la contribución de las instituciones del país, el nivel tecnológico a alcanzar y en él, los objetivos de investigación y desarrollo.
- La protección debe incluir: la de las infraestructuras críticas, incluidos los CIS, la protección de los ciudadanos y la protección del territorio nacional y sus instituciones.
- Debe incluir la previsión, prevención, disuasión, protección y reacción. No debe limitarse a acciones puramente defensivas o pasivas, sino que deben preverse capacidades ofensivas en el espacio cibernético o incluso en otros espacios de forma que disuadan de nuevos ataques.
- La ciberseguridad y, por lo tanto, la ciberdefensa deben enfocarse de forma que integren a las distintas agencias de seguridad e inteligencia del estado, los centros de investigación tanto públicos como privados y que coordinen con el sector privado y los propios ciudadanos. El impacto de una amenaza en el espacio cibernético tiene implicancias sociales y económicas en el país que la sufre.
- A nivel internacional, la ciberdefensa debe incluirse también en las estrategias de defensa colectiva.

EUROPA

Reino de España

En el caso de España, además de la Ley de Seguridad Nacional antes mencionada, se encuentra la Estrategia de Seguridad Nacional la cual,

> ...constituye el marco político estratégico de referencia de la Política de Seguridad Nacional. Contiene el análisis del entorno estratégico, concreta los riesgos y amenazas que afectan a la seguridad de España, define las líneas de acción estratégicas en cada ámbito de actuación y promueve la optimización de los recursos existentes. Se elabora a iniciativa del presidente del Gobierno, quien la somete a la aprobación del

228 Communications and Information Systems. Sistemas de Información y Telecomunicaciones que utilizan las TIC o Tecnologías de la Información (informática) y las Comunicaciones (telecomunicaciones).

Consejo de Ministros y se revisará cada cinco años o cuando lo aconsejen las circunstancias cambiantes del entorno estratégico[229].

La Estrategia de Seguridad Nacional[230],

...considera los ciberataques como una amenaza actual, real y en crecimiento para los intereses nacionales, haciendo hincapié en la necesidad de garantizar el uso seguro del espacio cibernético" pues "la ciberseguridad no es un mero aspecto técnico de la seguridad sino un eje fundamental de nuestra sociedad y sistema económico.

A partir de la estrategia de Seguridad, España elaboró la Estrategia de Ciberseguridad Nacional[231] en la cual se ponen de manifiesto la gravedad y complejidad de las ciberamenazas, así como el grado de organización alcanzado por los grupos delincuentes o terroristas que están detrás de ellas. También, se identifican la necesidad de coordinación entre los organismos públicos dedicados a la ciberseguridad, los dedicados a la ciberdefensa y la de estos con los actores técnicos, académicos, juristas y privados y se destaca la necesidad de la cooperación internacional, dado que la amenaza es de carácter global.

Para el Reino de España, la Estrategia de Ciberseguridad Nacional es el documento estratégico que sirve de fundamento al gobierno español, para "desarrollar las previsiones de la Estrategia de Seguridad Nacional en materia de protección del espacio cibernético con el fin de implantar de forma coherente y estructurada las acciones de prevención, defensa, detección y respuesta frente a las ciberamenazas".

Para alcanzar los objetivos señalados, la Estrategia de Ciberseguridad Nacional de España[232] se articula a través de una serie de líneas de acción, la primera de las cuales es la de "Incrementar las capacidades de prevención, defensa, detección, análisis, respuesta, recuperación y coordinación ante las ciberamenazas, haciendo énfasis en las Administraciones Públicas, las infraestructuras críticas, las capacidades militares y de defensa y otros sistemas de interés nacional".

Entre otras cosas, dicha línea de acción prevé:

- Ampliar y mejorar permanentemente las capacidades de Ciberdefensa de las Fuerzas Armadas que permitan una adecuada protección de sus redes y sistemas de información y telecomunicaciones, así como de otros sistemas que afecten a la Defensa Nacional. Se consolidará la implantación del Mando Conjunto de Ciberdefensa y se potenciará su cooperación con los diferentes órganos con capacidad de respuesta ante incidentes cibernéticos en aspectos de común interés.

---

229 España, Ley 36/2015, de 28 de septiembre, de Seguridad Nacional; Disponible en: http://noticias.juridicas.com/actualidad/noticias/10529-contenido-de-la-ley-36-2015-de-28-de-septiembre-de-seguridad-nacional/

230 Ibidem

231 España, Estrategia de Ciberseguridad Nacional 2013; Palacio de La Moncloa; P. 3; Disponible en: http://www.lamoncloa.gob.es/documents/20131332estrategiadeciberseguridadx.pdf

232 Ibidem; P. 31

› Potenciar las capacidades militares y de inteligencia para ejercer la respuesta oportuna, legítima y proporcionada en el espacio cibernético ante amenazas o agresiones que puedan afectar a la Defensa Nacional.

Para el caso que ocupa en esta obra, el objetivo de la Ciberseguridad de España[233], es el de "garantizar un uso seguro de las redes y los sistemas de información a través del fortalecimiento de las capacidades de prevención, detección y respuesta a los ciberataques".

=A un mismo nivel se encuentra la Directiva de Defensa Nacional de 2012 que dispone la participación del Ministerio de Defensa en el impulso de una gestión integral de la ciberseguridad, en el marco de los principios que se establecen al efecto en la Estrategia de Ciberseguridad Nacional. En función de ello, es que creó el Mando Conjunto de Ciberdefensa[234], cuyo "ámbito de actuación son las redes y los sistemas de información y telecomunicaciones de las Fuerzas Armadas, así como aquellas otras redes y sistemas que específicamente se le encomienden y que afecten a la Defensa Nacional".

De manera coherente con la Estrategia de Ciberseguridad Nacional y con la Directiva de Defensa Nacional, la Orden Ministerial que dispone la creación del Mando Conjunto de Ciberdefensa de las Fuerzas Armadas del Reino de España, le asigna como misión a dicho Comando la de:

> ...planificar y ejecutar las acciones relativas a la ciberdefensa militar en las redes y sistemas de información y telecomunicaciones de las Fuerzas Armadas u otros que pudiera tener encomendados, así como contribuir a la respuesta adecuada en el espacio cibernético ante amenazas o agresiones que puedan afectar a la Defensa Nacional.

En síntesis, por medio de estas normas, España pretende incrementar las capacidades de prevención, defensa, detección, análisis, respuesta, recuperación y coordinación ante las ciberamenazas, haciendo énfasis en las Administraciones Públicas, las infraestructuras críticas, las capacidades militares y de Defensa y otros sistemas de interés nacional[235] mediante la cooperación de los organismos con responsabilidades en ciberseguridad, en especial entre el CERT[236] de la Administración Pública del Centro Criptológico Nacional (CCN-CERT), el Mando Conjunto de Ciberdefensa de las Fuerzas Armadas (MCCD) y el CERT de Seguridad e Industria[237].

---

233 Ibidem P. 42

234 España. Ministerio de Defensa, Orden Ministerial 10/2013, de 19 de febrero, Disponible en: http://www.ieee.es/Galerias/fichero/Varios/BOD_26.02.2013_MandoConjuntoCiberdefensa.pdf .

235 Ibidem.

236 Equipo de Respuesta ante Emergencias Informáticas (CERT, del inglés Computer Emergency Response Team)

237 En la República Argentina dicha coordinación se lleva a cabo a través del denominado Ejercicio Nacional de Respuestas a Incidentes Cibernéticos (ENRIC) en el marco del Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad cuyo objetivo es actualizar los conocimientos sobre los canales de comunicación e intercambio de información ante un eventual incidente cibernético. Más información puede verse en Internet http://www.gacetamarinera.com.ar/nota.asp?idNota=6643 .

República de Francia

En el caso de Francia, en el Libro Blanco de la Seguridad y la Defensa de 2008, se puso de relieve como nueva amenaza, el espacio cibernético, centrándose en la seguridad de los "sistemas de información, centros nerviosos reales de nuestra sociedad", donde "todos los sectores de actividades, ya sean estatales, industriales, financieras o comerciales, dependen más de la tecnología y redes de comunicaciones electrónicas"[238].

Esa apreciación distingue tres escenarios principales:

- un ataque contra los sistemas informatizados que gestionan infraestructuras críticas como plantas nucleares, red ferroviaria o aeropuertos que pudiesen provocar destrozos similares o superiores a los de un bombardeo físico.
- un ataque contra la parte visible de Internet, esto es, las webs y las intranets de administraciones clave, como presidencia, policía, impuestos y hospitales con la consiguiente provocación de un caos y desprestigio del Estado ante sus ciudadanos y ante las potencias extranjeras.
- la integración de cualquiera de esos ataques informáticos en el marco de una secuencia clásica de guerra convencional.

A mediados de 2009 se creó la Agencia Nacional para la Seguridad de Sistemas de Información (ANSSI) con la misión de proteger los sistemas nacionales de información y proponer las normas que debían aplicarse para la protección de los sistemas estatales y verificar la aplicación de las medidas adoptadas. Por medio del Centro Operacional de la Seguridad de Sistemas de Información (COSSI), se detectarían y responderían los ataques, se vigilarían las redes más sensibles de la administración y se desarrollarían nuevas capacidades defensivas.

El estatuto de la ANSSI se reforzó a principios de 2011, puesto que la agencia pasó a ser la autoridad nacional de defensa de los sistemas de información. Luego de la creación de la ANSSI, Francia publicó en febrero de 2011 una Estrategia Nacional de Defensa y Seguridad de los Sistemas de Información y en el Libro Blanco de 2013 identificó la amenaza de sabotaje de las infraestructuras críticas[239].

En febrero de 2011, la ANSSI presentó la Estrategia Nacional de Ciberseguridad de Francia[240]. Sobre la base de lo establecido en su Libro Blanco de Defensa y la Seguridad, el documento establece cuatro objetivos:

1. Convertir a Francia en una potencia mundial en defensa cibernética con mantenimiento de su independencia estratégica y trabajar para asegurarse que pertenece al círculo íntimo de las naciones líderes en el ámbito de la defensa cibernética,

---

238 Ortiz, Javier Ulises (2012). Estrategias de Defensa Cibernética en la Era de la Información. Revista ESG, Nro 582. Bs As.

239 Francia, Libro Blanco de la Defensa y Seguridad de Francia 2013, Disponible en: http://www.diplomatie.gouv.fr/fr/politique-etrangere-de-la-france/defense-et-securite/la-defensenationale/article/livre-blanc-sur-la-defense-et-la-106560.

240 Francia, Estrategia Nacional de Ciberseguridad, 2011 Disponible en: https://www.enisa.europa.eu/media/news-items/Information_system_security_France_strategy.pdf.

a la vez que se procure multiplicar la cooperación tanto a nivel operacional y en la aplicación de una estrategia unificada para hacer frente a amenazas comunes.
2. Salvaguardar la capacidad de Francia para tomar decisiones a través de la protección de la información relacionada con su soberanía y las autoridades gubernamentales y actores de gestión de crisis deben disponer de los recursos para comunicarse en cualquier situación y en total confidencialidad por medio de redes que cumplan con esta necesidad, en particular a nivel local, lo que garantice la confidencialidad de la información que circula por ellas.
3. Fortalecer la ciberseguridad de las infraestructuras nacionales críticas para que funcionen correctamente, en las que la sociedad es cada vez más dependiente de sistemas de información y redes, en particular Internet. Evitar cualquier ataque con éxito sobre un sistema de información crítico de Francia que pudiera tener consecuencias económicas graves o humanas. Estrechar la colaboración con los fabricantes y operadores de equipos pertinentes para que el estado garantice y mejore la seguridad de estos sistemas críticos.
4. Garantizar la seguridad en el espacio cibernético en el que las amenazas a los sistemas de información afectan simultáneamente los servicios públicos, privados, empresas y ciudadanos. Los servicios públicos deben operar de manera ejemplar y mejorar la protección de los sistemas de información y los datos que se les encomienden.

Para cumplir estos objetivos, la estrategia identificó siete áreas de acción:

1. Anticipar y analizar el espacio cibernético para la efectiva toma de decisiones
2. Detectar y bloquear ataques, estar alerta y apoyar a las víctimas potenciales
3. Mejorar y mantener medios humanos, científicos, técnicos, industriales y las capacidades con el fin de mantener independencia
4. Proteger los sistemas de información del Estado y los operadores de infraestructuras críticas para garantizar una mejor capacidad de recuperación nacional
5. Adaptar la legislación francesa para incorporar los avances tecnológicos y nuevas prácticas
6. Desarrollar iniciativas de colaboración internacional en las áreas de información, sistemas de seguridad, ciberdefensa y lucha contra la delincuencia informática con el fin de proteger los sistemas de información nacionales
7. Comunicar, informar y convencer para aumentar la comprensión por parte de la población, de la magnitud de los desafíos relacionados con la seguridad en los sistemas

Por su parte, el Secretario General de la Defensa y la Seguridad Nacional mantiene dos planes de trabajo[241]: el Plan *Vigipirate* de vigilancia, prevención y protección, cuyo principal objetivo es la preparación del estado para la protección de la población, su in-

241 Francia. Secretaría General de la Defensa y Seguridad, Oficina del Primer Ministro; Disponible en: http://www.sgdsn.gouv.fr/site_rubrique98.html.

fraestructura y sus instituciones, y el Plan *Piranet*, complementario al anterior, que funciona en respuesta a amenazas o ataques a gran escala -utilizando medios específicos de agresión- o en situaciones que afectan a los entornos particulares donde se requiere la intervención del estado en una crisis de gravedad y se constituye así en uno de los pilares de la estrategia de esa defensa. Cabe destacar que en 2012 se estableció en la Escuela Interarmas del Ejército Francés un centro de conocimientos de ciberdefensa[242].

En febrero de 2014, el Ministerio de Defensa de Francia elaboró el denominado *Pacte Défense Cyber*[243] que pone en perspectiva todo el trabajo realizado por el Ministerio de Defensa y que, a través de 50 acciones, divididas en seis ejes, proporciona los fundamentos para el fortalecimiento de la base industrial de defensa y de las tecnologías de seguridad nacional y, también, un conjunto de medidas para crear o apoyar proyectos de los gobiernos locales, de las grandes empresas, de las PYME, y de cualquier otra organización que requiera medios cibernéticos.

En este documento se fijan seis objetivos:

1. Fortalecer el nivel de seguridad de los sistemas de información y medios de defensa y de intervención del Ministerio de Defensa y sus principales socios de confianza
2. Prepararse para el futuro para intensificar el esfuerzo de investigación, tanto técnica y académica como operacional, apoyada en base industrial
3. Reforzar los recursos humanos dedicados a la ciberdefensa y construir las carreras profesionales asociadas
4. Desarrollar el centro de excelencia en ciberdefensa en Bretaña en beneficio del Ministerio de Defensa y la comunidad nacional de ciberdefensa
5. Cultivar una red de socios extranjeros, en Europa y en la Alianza Atlántica y en áreas de interés estratégico
6. Favorecer la aparición de una comunidad nacional de ciberdefensa confiando en un círculo de socios y redes de la reserva

El 16 de octubre de 2015 Manuel Valls, Primer Ministro francés, dio a conocer la Estrategia Nacional para la Seguridad en el ámbito digital. El documento, coordinado por la ANSSI establece y actualiza objetivos para el Secretario de la Defensa y la Seguridad Nacional y responde a los nuevos desafíos que nacen de la evolución de los usos digitales y amenazas que se relacionan con cinco objetivos[244]:

1. Garantizar la soberanía nacional defendiendo los intereses fundamentales, defensa y seguridad de los sistemas de información del estado y de las infraestructu-

242 Defense Systems, France moves to boost cyber warfare skills among officer corps, julio 5 2012; Disponible en: http://defensesystems.com/articles/2012/07/05/agg-france-cyber-warfare-officer-training.aspx

243 Ministere de la Defense (página web del Ministerio de Defensa de Francia) Disponible en: http://www.defense.gouv.fr/actualites/articles/presentation-du-pacte-defense-cyber

244 Anssi Agencie Nacionale de la Securite de Sytemes d´information; Disponible en: http://www.ssi.gouv.fr/.

ras críticas frente a una crisis informática y desarrollar un pensamiento estratégico autónomo, respaldado por un conocimiento técnico de primer nivel. Crear un dispositivo para defender los intereses fundamentales en el espacio cibernético del futuro y reforzar la seguridad de las redes críticas y su capacidad de resistencia en caso de un ataque grave mediante el desarrollo de cooperaciones tanto a escala nacional con actores privados como a escala internacional.

2. Tener una fuerte respuesta contra ciberactos maliciosos proveyendo medidas de protección y de reacción que otorguen confianza digital, privacidad de datos personales frente a ciberataques para todo tipo de empresas y para los particulares. La protección implicará una mayor vigilancia de los poderes públicos en el uso de los datos personales y el desarrollo de una oferta de productos de seguridad digital adaptada al público en general. La reacción se articulará en torno a un dispositivo de asistencia a las víctimas de ciberataques que brindará una respuesta técnica y judicial a tales actos.
3. Informar al público en general, sensibilizando en la materia y formando y sensibilizando a los colegiales y estudiantes. Además, con el fin de dar respuesta a la creciente demanda de empresas y administraciones en materia de ciberseguridad, se desarrollará la formación de expertos en este ámbito.
4. Hacer de la seguridad digital una ventaja competitiva para las empresas francesas y fortalecer la voz de Francia en el extranjero, lo que propicie un entorno de las empresas del sector digital, política industrial, de exportación e internacionalización. El crecimiento de los mercados del sector digital a escala mundial y el consiguiente aumento de las exigencias de seguridad constituyen una oportunidad de diferenciación para los productos y servicios franceses que dispongan de un nivel de seguridad digital adaptada a los usos. A través del apoyo a la inversión, propiciar la innovación y la exportación, pero también a través de la contratación pública, donde el estado desarrollará un entorno propicio a las empresas francesas del sector digital que propondrá una oferta de productos y servicios seguros.
5. Buscar una Europa con soberanía digital y estabilidad del espacio cibernético. La regulación de las relaciones en el espacio cibernético se ha convertido en un tema de suma importancia en las relaciones internacionales. Francia promoverá, junto con los estados miembro que así lo deseen, una hoja de ruta para la soberanía digital de Europa. Reforzará asimismo su influencia en las instancias internacionales y respaldará a los países voluntarios menos protegidos en la implementación de dispositivos de ciberseguridad con el fin de contribuir a la seguridad global del espacio cibernético.

Luego de la ocurrencia de los atentados terroristas de París, el Presidente Hollande en su mensaje a la Asamblea Nacional del 16 de noviembre de 2015 expuso que "el Ejército francés aumentará su despliegue en ciberdefensa durante los próximos cuatro años, hasta 2019" y que se aumentarán las medidas en torno al control de las comunicaciones electrónicas, ya que no se puede luchar en estado de guerra contra lo que se tenía hace años.

Reino Unido de Gran Bretaña

En 2010, el gobierno británico crea el Consejo Nacional de Seguridad y promulga la denominada Estrategia Nacional de Seguridad en la cual se considera a "los actos hostiles en el espacio cibernético contra Gran Bretaña llevados a cabo por otros estados o por el ciberdelito a gran escala" como uno de los cuatro grupos de riesgo de más alta prioridad para la seguridad nacional debido a su posibilidad de ocurrencia y a su impacto[245].

En noviembre de 2011, el Reino Unido consideró el carácter estratégico de su Ciberseguridad y publicó la correspondiente estrategia: *The UK Cyber Security Strategy Protecting and promoting the UK in a digital world.*

En la denominada *"National Security Strategy and Strategic Defence and Security Review 2015 A Secure and Prosperous United Kingdom"* promulgada en noviembre de 2015, al mismo tiempo que se describe la manera en que se equiparan las Fuerzas Armadas, la policía y las agencias de inteligencia para hacer frente a las amenazas actuales y futuras[246], se establece que una de las misiones de las fuerzas armadas británicas será la de defender y contribuir a la seguridad del Reino Unido y sus territorios de ultramar, lo cual incluye la disuasión de ataques, la defensa del espacio aéreo, las aguas territoriales y el espacio cibernético, la lucha contra el terrorismo en el país y en el extranjero; el apoyo a las autoridades civiles del Reino Unido en el fortalecimiento de la resiliencia[247]; y la protección de los ciudadanos británicos en el extranjero.

En tal sentido, Gran Bretaña cuenta con el Programa Nacional de Seguridad Cibernética, tendiente a ampliar los sistemas de protección de la seguridad cibernética, asegurando la información (*Information Assurance*); mejorando la detección y el análisis de los ataques cibernéticos; aumentando la cooperación con países aliados; y creando una unidad cibernética conjunta, en colaboración con el Ministerio de Defensa, para desarrollar nuevas tácticas, técnicas y planes relativos a las operaciones militares.

Estados Unidos de Norteamérica

La primera referencia al desafío cibernético puede verificarse en la Estrategia Nacional para Asegurar el Espacio Cibernético de Estados Unidos -de febrero de 2003-, del entonces presidente George W. Bush. Esta estrategia es un componente de implementación de la Estrategia Nacional para la Seguridad Interna y está complementada por la Estrategia Nacional para la Protección Física de Infraestructura Crítica y Bienes Clave[248].

---

245 A Strong Britain in an Age of Uncertainty: The National Security Strategy; P. 27 Disponible en: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/61936/national-securitystrategy.pdf.

246 National Security Strategy and Strategic Defence and Security Review 2015 A Secure and Prosperous United Kingdom, Foreword; Disponible en: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/478933/52309_Cm_9161_NSS_SD_Review_web_only.pdf.

247 Resiliencia es la capacidad de un material, mecanismo o sistema para recuperar su estado inicial cuando ha cesado la perturbación a la que había estado sometido. Por lo tanto, la defensa informática debería ser resiliente, es decir permitir recuperar las capacidades que se pueden perder ante un ataque cibernético.

248 National Security Council, The National Strategy to Secure Cyberspace, Feb 2003; Disponible en: https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf

La Estrategia de Seguridad Nacional de Estados Unidos, publicada en mayo de 2010 por la Casa Blanca, destaca igualmente la amenaza del espacio cibernético contra Estados Unidos y determina que: "Las capacidades espaciales y ciberespaciales que alimentan nuestra vida cotidiana y las operaciones militares son vulnerables a la interrupción y al ataque". En este Informe de la Estrategia de Seguridad Nacional del presidente Obama, la palabra *"cyber"* ya sea como sustantivo o adjetivo, aparece mencionada 24 veces. La reiteración de este término puede interpretarse como la creciente importancia de un aspecto del conflicto hasta ese momento sin mayores preocupaciones de seguridad nacional, ya que, en la edición anterior, publicada en marzo del 2006, se lo menciona solo una vez.

En este documento es donde por primera vez aparece el término espacio cibernético, cuyas amenazas "representan uno de los más graves de seguridad nacional, la seguridad pública, y los desafíos económicos que enfrentamos como nación." Para disuadir, prevenir, detectar, defenderse y recuperarse rápidamente de intrusiones y ataques cibernéticos, se deberá invertir en el sector privado, en gente y tecnología, así como en la tarea de buscar asociados nacionales, internacionales, públicos y privados[249]. A esta altura de los hechos, se siguen dos políticas; invertir en gente y tecnología, y buscar aliados.

Un ejemplo de la dependencia militar del espacio cibernético en Estados Unidos lo constituye la Global Information Grid (GIG), que contiene una amplia gama de medios de comunicación, que incluye satélites, desplegados alrededor del mundo. La red habilita a los Estados Unidos para transmitir información, órdenes a sus tropas, guiar bombas inteligentes a los objetivos utilizando GPS o controlar vehículos aéreos no tripulados en forma rápida, fiable y segura. Si se llegaba a dañar esta red, los Estados Unidos corrían el riesgo de perder el dominio que actualmente detentan en los campos de batalla de todo el mundo[250].

En el año 2011, la Casa Blanca publicó la *International Strategy for Cyberspace*[251], que es una agenda sobre los nuevos desafíos de esta especie para dar a conocer las prioridades de las políticas de Estados Unidos. Estas prioridades abarcan la economía, la protección de las propias redes, el cumplimiento de la ley, los aspectos militares, la gobernanza de Internet, el desarrollo internacional y la libertad en el uso de Internet.

En la Estrategia Nacional Militar del 2011 se hace referencia con claridad a la amenaza cibernética[252]. Es en febrero de ese año que el Vice Secretario de Defensa de Estados Unidos enumeró tres amenazas cibernéticas: explotación de redes, interrupción de redes y sabotaje con propósito de destrucción. En noviembre de ese mismo año, la Agencia de Proyectos de Investigación de Defensa Avanzados (DARPA) organizó un seminario

249 The White House, The National Security Strategy Report, May 2010, página 8; Disponible en: http://nssarchive.us/NSSR/2010.pdf .

250 Shmuel Even y David Siman Tov, Cyberwarfare, Concepts and Strategic Trends, The Institute for National Security Studies, Ramat Aviv, Tel Aviv, Mayo 2012, Página 48, Disponible en: http://www.isn.ethz.ch/Digital-Library/Publications/Detail/?id=152953

251 The White House, International Strategy for Cyberspace 2011; Disponible en: https://info.publicintelligence.net/WH-InternationalCyberspace.pdf

252 DoD, The National Military Strategy 2011; Disponible en: https://www.scribd.com/.../2011-NationalMilitary-Strategy-of-USA fecha de consulta 22 Diciembre 2015.

para determinar las frecuentes vulnerabilidades en las redes de defensa del Pentágono, y llegó a la conclusión que se carecía de capacidad para defender esas redes[253].

En la Política de Defensa para el hemisferio Occidental del año 2012, firmada por el presidente Obama, se hace referencia a la necesidad de hacer frente a las amenazas del espacio cibernético y la necesidad de que todos los países formen alianzas e integrar esfuerzos para hacer frente a estas[254]. Nótese que a las amenazas cibernéticas se las consideran dentro del área de defensa.

En el Informe de la Estrategia Nacional de Seguridad de 2015[255], se refiere a los espacios como: el terrestre, marítimo, aéreo, espacial y cibernético, como espacios compartidos. Se ha tenido acceso también a la *US. Coast Guard Cyberstrategy* 2015 que contiene aspectos específicos para la conducción de esta fuerza de seguridad en administrar los riesgos cibernéticos en la infraestructura marítima[256].

El organismo responsable de proporcionar una visión global y una estrategia de defensa del espacio cibernético es la Casa Blanca. Al lado del Presidente se encuentra el Coordinador de Seguridad Cibernética y Asistente Especial del Presidente. Tiene la responsabilidad de coordinar y sincronizar las políticas de administración y asistir al Presidente en la gestión de las crisis en la seguridad del espacio cibernético.

La División Nacional de Seguridad Cibernética se encuentra dentro del Departamento de Seguridad Interna (*Homeland Security Command*) y es la entidad específica a cargo de la implementación de la estrategia en el espacio cibernético. Su atención se centra en la seguridad de las redes federales y la protección de las infraestructuras críticas. Está a cargo de la implementación del Sistema Nacional de Respuesta en el Espacio cibernético que coordina cuestiones administrativas, procedimientos y protocolos en caso de eventos inusuales en el espacio cibernético. Por otra parte, la división es responsable del Programa de Gestión de Riesgo Cibernético, diseñado para identificar los riesgos y reducirlos y utiliza consideraciones de costo-beneficio. La División trata de la coordinación entre las autoridades oficiales del estado y con el intercambio de información entre diversas instituciones y organismos (lo que incluye el intercambio con el sector privado), y también se centra en la alerta temprana sobre actividades hostiles en el espacio cibernético. Existe también una cooperación estrecha entre la División y el Comando Cibernético de Estados Unidos (CYBERCOM) en el Departamento de Defensa de este país.

El Departamento de Defensa está a cargo de la ofensiva y defensiva cibernética y de asistir a las organizaciones civiles. Para cumplir con esta finalidad, se estableció el *US CYBERCOM* en mayo de 2010, como parte de la estructura de comando del Pentágono.

---

253 Ackerman, Spence, "Darpa Begs Hackers: Secure our Networks," November 7, 2011; Disponible en: http://www.wired.com/dangerroom/2011/11/darpa-hackers-cybersecurit

254 US Department of Defense, Política de Defensa para el hemisferio occidental; octubre 2012, P. 12

255 White House, National Security Strategy Report 2015; Disponible en: https://www.whitehouse.gov/sites/default/files/docs/2015_national_security_strategy.pdf

256 US Cyber Coast Guard Strategy June 2015; Disponible en: http://www.uscg.mil/seniorleadership/DOCS/cyber.pdf

Este Comando Estratégico está subordinado al *Strategic Command* (US STRATCOM) y es el responsable de llevar a cabo misiones[257] en el espacio cibernético para asegurar la libertad de acción en este y reducir las amenazas a la seguridad nacional.

Son sus funciones[258] estar a cargo de la protección de todas las redes militares y del Departamento de Defensa; crear una única y clara cadena de comando para alcanzar decisiones de guerra cibernética: del Presidente de los Estados Unidos al Secretario de Defensa, al Comandante del Comando Estratégico, al Comandante del Comando Cibernético y hasta las unidades militares individuales a lo largo y ancho del mundo; crear alianzas con elementos fuera del ámbito militar y el Departamento de Defensa (y con otros departamentos de gobierno y el sector privado) y fuera de los Estados Unidos, para compartir información acerca de amenazas y hacer frente a vulnerabilidades compartidas producto de amenazas cibernéticas. Operacionalmente, integrar las misiones en el espacio cibernético y sincronizar los efectos en el ambiente global de seguridad, para implementar una sucesión de misiones en el espacio cibernético; crear alertas de misiones en el espacio cibernético contra los Estados Unidos y emitir alertas sobre enemigos; asimismo ser el representante militar en el espacio cibernético en comunicaciones con varios elementos, lo que incluye otras organizaciones de defensa, así como compañías estadounidenses y extranjeras.

La comunidad de inteligencia es el componente más importante en el conjunto de los organismos para la defensa del espacio cibernético norteamericano. El documento de la comunidad de inteligencia de 2014 muestra que el fortalecimiento de capacidades del espacio cibernético es una de las primeras cinco tareas más importantes de la actualidad que deben enfrentar las agencias de inteligencia estadounidenses.

Actualmente, el Ejército y la comunidad de inteligencia están redoblando sus esfuerzos para desarrollar las capacidades de guerra cibernética. Podría ser que esta tendencia requiera - ahora y posiblemente en el futuro - la división formal de la responsabilidad y la autoridad para la guerra cibernética entre los organismos. Se debe tener en cuenta que la *National Security Agency* (NSA) es parte de la comunidad de inteligencia estadounidense, así como parte del Ejército y el Departamento de Defensa. También, que el Comandante del *US CYBERCOMAND* es a la vez el Asesor de Seguridad Nacional y director de la NSA.

En el año 2015, el Departamento de Defensa publicó su Ciber Estrategia de Defensa[259]. Queda en evidencia que el espacio cibernético debería ser tratado como un dominio al igual que el mar, la tierra, el aire y el espacio. Tratar el espacio cibernético como un dominio significa que los militares deben operar en él de una manera similar a la que lo

---

257 En el nivel estratégico una misión se expresa como una tarea con un propósito.

258 Estas funciones fueron enunciadas por el primer Comandante del US CYBERCOM LTG Alexander US Director of National Intelligence, The National Intelligence Strategy of the USA, DNI Office, August 2014; Disponible en: https://www.dni.gov/files/documents/2014_NIS_Publication.pdf

259 US DoD, Cyberstrategy 2015; Disponible en: http://www.defense.gov/Portals/1/features/2015/0415_cyber-tragey/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf

hacen en los tradicionales y que deben organizar, entrenar y equiparse para llevar a cabo misiones cibernéticas.

En ese documento se sostiene que hay que emplear nuevos conceptos de defensa para proteger las redes y sistemas del Departamento de Defensa. A diferencia de las defensas pasivas que emplean solamente después de la notificación y detección de los hechos (basado en servidores de seguridad), las defensas activas se basan en un enfoque dinámico. Las defensas activas funcionan sobre la base de la velocidad de la red, el uso de sensores, software y firmas derivadas de inteligencia para detectar y detener cualquier código malicioso antes de que cause cualquier daño.

Todo ello se fundamenta en tres líneas de "resistencia": las dos primeras se apoyan en los principios de las mejores prácticas comerciales, la protección ordinaria de computadoras como antivirus, antimalware y firewalls. La tercera línea, en la capacidad de inteligencia del gobierno. La función de esta capa es proporcionar defensas activas altamente especializadas, para transmitir información acerca de los ataques desde los sensores externos hasta los mecanismos de defensa, coordinar las fuerzas que operan en el espacio cibernético de la nación y gestionar la batalla sobre la base de una visión global.

La cooperación cívico militar es indispensable ya que se hace necesario asegurar el espacio cibernético civil y la infraestructura, sin la cual la red eléctrica y las oficinas del gobierno no pueden funcionar.

Por otra parte, en noviembre de 2011, como parte del Acta Autorización de Defensa 2011, el Departamento de Defensa informó que Estados Unidos se reserva el derecho a tomar represalias militarmente ante "ciberataques significativos dirigidos contra los Estados Unidos, la economía, el gobierno o las fuerzas militares" y aquí se autoriza el uso de operaciones cibernéticas ofensivas[260].

El *USCYBERCOM*, desde su creación, ha sufrido un proceso de transformación y llegó en la actualidad a focalizar su misión en definir y lograr los objetivos estratégicos. Para ello, ha delegado las áreas de misión del nivel operacional en tres distintas fuerzas[261]: la primera de ellas es la *Cyber National Mission Force* (CNMF), que defiende a los Estados Unidos y sus intereses contra los ataques cibernéticos estratégicos. La segunda consta de cuatro comandos conjuntos diferentes (JFHQs) además del *Coast Guard Cyber Command* (CGCYBER) para apoyar a los comandos combatientes geográficos y a los comandos funcionales en todo el mundo. La base del JFHQ-Cyber son los cibercomponentes de cada una de las fuerzas armadas – el *Army Cyber Command* (ARCYBER), el *Fleet Cyber Command* (FLTCYBER), el *Marine Corps Cyberspace Command* (MARFORCYBER), y el *Air Forces Cyber* (AFCYBER) – que constituyen el primer paso vital para integrar las operaciones en el espacio cibernético y, de esa manera, conseguir los efectos en apoyo de comandantes combatientes. La tercera fuerza, y la más reciente, es la JFHQ-DODIN, la cual proporciona unidad de comando y de

260 US DoD "DOD Report Cyber Attacks Could Elicit Military Response," November 16, 2011; Disponible en: http://www.infosecisland.com/blogview/18218-DoD-Report-Cyber-Attacks-Could-Elicit-MilitaryResponse.html.

261 Joint Forces Quarterly 80; 1st Quarter 2016, Beyond the Build: How the Component Commands Support the U.S. Cyber Command Vision; Compiled by the U.S. Cyber Command Combined Action Group; P. 86 Disponible en: http://ndupress.ndu.edu/JFQ/Joint-Force-Quarterly-80/.

esfuerzo para asegurar, operar y defender la Red de Información del Departamento de Defensa (DODIN).

Durante el trienio 2013-2015, el Pentágono invirtió 23.000 millones de dólares en mejorar la resiliencia de la infraestructura TIC del Pentágono, en la adquisición de nuevas capacidades cibernéticas destinadas al USCYBERCOM y en aumentar el número de efectivos del comando desde los 900 miembros existentes a principios de 2013 hasta los cerca de 5.000 previstos para finales de 2015.

Según Fojón Chamorro[262],

> En marzo de 2016, inspirándose en programas similares llevados a cabo por grandes compañías tecnológicas de los Estados Unidos, el Pentágono anunciaba la convocatoria del primer *Bug Bounty*[263] en la historia de la administración del país. Bajo el elocuente título de "*Hack the Pentagon*", el entonces Secretario de Defensa Ash Carter retaba a los hackers estadounidenses a reportar los fallos de seguridad que detectasen en los sitios webs dependientes del Departamento de Defensa. Durante 20 días, 1.400 hackers – entre los que se encontraban profesionales de las TIC, profesores universitarios e incluso estudiantes de bachillerato- siguieron las reglas impuestas por el Departamento de Defensa para probar la seguridad de parte del ciberespacio militar estadounidense. Cientos de bugs fueron reportados - el primero de ellos a los trece minutos de comenzar el reto - y más de 75.000 dólares repartidos entre los expertos que reportaron fallos de seguridad relevantes.

Para Fojón, "Este tipo de eventos está posibilitando que el Pentágono integre profesionales, procesos y tecnologías innovadoras en la seguridad y defensa de su ciberespacio específico" y, a su vez,

> Iniciativas como "*Hack the Pentagon*" no solo posibilitan la resolución de incidentes de seguridad en parte del ciberespacio militar estadounidense, sino que además permiten identificar y captar talento en el ámbito de la ciberdefensa nacional; a la vez que es una excelente oportunidad para reclutar expertos cualificados que formen parte de los "*red teams*" destinados a mantener la operatividad de las Fuerzas Armadas del país, cada vez más dependiente del ámbito ciber.

Por su parte, en abril de ese año, en su informe anual ante el Comité de Defensa del Senado, el Almirante Michael S. Rogers[264], Comandante del *USCYBERCOM* expresó

---

262 Fojón Chamorro, Enrique, Comentario Ciberelcano: Hackear el Pentágono, Informe mensual de ciberseguridad mayo 2017; Disponible en: http://www.realinstitutoelcano.org/wps/wcm/connect/0e682909-e55b-4bfd-b1be-50a2fe7602bd/Ciber_elcano_Num25.pdf?MOD=AJPERES&CACHEID=0e682909-e55b-4bfd-b1be-50a2fe7602bd

263 Bug Bounty: programas muy comunes en el ámbito de la seguridad que ofrecen recompensas monetarias y reconocimiento a quienes encuentren vulnerabilidades en sistemas, sitios y redes.

264 Statement of Admiral Michael S. Rogers Commander United States Cyber Command Before the Senate Armed Services Committee 5 April 2016 Disponible en: Https://Www.Armed-Services.Senate.Gov/Imo/Media/Doc/Rogers_04-05-16.Pdf

"Ahora contamos con 123 equipos de un total previsto de 133; estos equipos comprenden 4.990 personas y llegarán a 6.187 cuando terminemos. En términos de progreso, contamos con 27 equipos que hoy están plenamente operativos y 68 que han alcanzado una capacidad operativa inicial".

Entre otros conceptos expresó "La defensa de América en el ciberespacio es un esfuerzo conjunto del gobierno, realmente de toda la Nación. Ninguna agencia o departamento tiene la autoridad, información o sabiduría para cumplir sola con esta misión, razón por la cual USCYBERCOM y NSA recientemente actualizaron nuestras empatías con el Departamento de Seguridad Nacional en un plan de acción cibernética para diagramar nuestra colaboración".

Finalmente cabe agregar que el 10 de mayo de 2017 el Presidente Donald Trump promulgó la Orden Ejecutiva[265] "*Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*" y llamó a secretarios de gabinete y a los jefes de distintas agencias federales a seguir las normas para mejorar la ciberseguridad de infraestructura crítica, elaboradas por el Instituto Nacional de Estándares y Tecnología durante la administración del ex Presidente Barack Obama[266].

> La orden ejecutiva detalla tres temas principales que son de particular interés porque sugieren importantes nuevos desarrollos en el enfoque del gobierno federal para la seguridad cibernética. La orden destaca la ciber-disuasión, es decir, el proceso de desalentar a potenciales atacantes e identifica la necesidad de fortalecer la seguridad de la red eléctrica y las capacidades bélicas de los militares[267].

ASIA

China

La Ley de Ciberseguridad de China fue promulgada el 7 de noviembre de 2016. Se tiene conocimiento de ella por un Boletín Informativo del Instituto de Estudios Estratégicos de España del 4 de enero de 2017, en un artículo firmado por David Ramírez Morán[268].

> Esta ley regula, en tan solo 79 artículos, aspectos tan dispares como la protección de datos, las obligaciones de las empresas e incluso las posibles sanciones a aplicar, para lo que, en otros países, son necesarias varias leyes, reglamentos y códigos. Esta brevedad se consigue mediante una ambigüedad que se presta a la interpretación y

---

265 White House; Executive Order "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure" Disponible en: https://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal

266 The conversation; Global ransomware attack reinforces message of Trump's new cybersecurity order; May 11, 2017; Disponible en: http://theconversation.com/global-ransomware-attack-reinforces-message-of-trumps-new-cybersecurity-order-72239

267 Ibidem

268 Ramírez Morán, Davis. Ciberseguridad en China. Publicado en la página web del Ministerio de Defensa de España el 04 de enero de 2017; Disponible en: http://www.ieee.es/contenido/noticias/2017/01/DIEEE101-2017.html. La cita es textual

que dota a su vez al Gobierno chino de mecanismos para la monitorización, la censura o el proteccionismo que han generado reacciones por parte de organizaciones de defensa de derechos humanos, así como de las multinacionales del sector. Las cuestiones sobre derechos y obligaciones de ciudadanos y empresas se abordan desde una aproximación que centraliza la responsabilidad en el Estado, en línea con el modelo de gobernanza del ciberespacio que el país promueve internacionalmente, frente al modelo de cooperación público privada que promueven las normativas comparables de otros países.

El primer escollo para interpretar esta ley es el idioma porque el texto está en chino y no hay traducción a ningún otro idioma. El texto incluye referencias explícitas al sistema político chino con la "*diseminación de los principales valores socialistas*" y en el Art. 12 prohíbe que la red sea usada para actividades que "inciten a la subversión de la soberanía nacional, la caída del sistema socialista, o mine la unidad nacional...". La ley persigue regular en forma general la seguridad de la información. El criterio para legislar es abordar el componente principal en forma transversal en los aspectos de Protección de Datos, Ley de los Servicios UTI, Ley General de Telecomunicaciones, Ley de Protección de Infraestructuras Criticas, Código Civil, Código Penal, Esquema General de seguridad y Estrategia de Ciberseguridad.

El Capítulo 4 de la Ley se refiere a la Seguridad en red, y el Capítulo 5 a Monitorización, Alerta temprana y Respuesta a incidentes. En el Capítulo sobre Marco Legal, a las empresas se les impone sanciones como cierre de páginas web, interrupción de las actividades de la empresa y cancelación de permisos y licencias y para las personas, sanciones que van hasta la prohibición en vida de operar en red.

En cuanto a los cibernautas, la libertad de expresión está vedada por la prohibición de tratar ciertos temas. Los registros de la red deben guardarse por seis meses. El denominado *Golden Shield* es el conjunto de infraestructuras con que el gobierno impide la conexión a ciertas páginas web. Eso ha dado lugar a una competencia entre las empresas que se conectan en forma cifrada. Las capacidades tecnológicas del *Golden Shield* se usaron para atacar a varias páginas web, con gran potencia en los ataques DoS atribuidos.

En cuanto a la seguridad de sus sistemas, los equipamientos críticos deben estar revisados y aprobados por expertos antes de ser distribuidos, así como se establece una medida para que se actualicen el software y el hardware para evitar "agujeros" de seguridad. La implementación de medidas de protección, la obligación de informar ante un ataque, el almacenamiento de los metadatos[269] de comunicaciones, el fomento de compartir los datos entre organismos y organizaciones, y la necesidad de concientización de usuarios y profesionales. Los contenidos que aparecen en esta ley son aquellos que preocupan a los estados que quieren un modelo depositado en las partes interesadas. Habrá que determinar la autoridad encargada de imponer las leyes, así como el órgano

269 Metadatos: La definición más simple sería: "Son los datos sobre los datos". Por ejemplo, las fichas de una biblioteca (metadatos) y los libros (datos). Mientras que las fichas tienen toda la información relacionada con el autor, el título, el ISBN, el año, la editorial, en el libro está el contenido que normalmente un usuario buscará.

responsable de garantizar los derechos e infraestructuras necesarias cuando surjan las principales diferencias.

Merece ser dicho que la guerra entre China y Google continúa dando sus coletazos. Mientras que la compañía californiana acusa al régimen chino de censura, el gigante asiático prosigue con su estrategia de contraatacar creando sus propias herramientas en Internet para combatir el impacto de los de Google. El último movimiento ha sido el lanzamiento de su propio buscador. Se llama *Goso* y pretende hacer frente al liderazgo de Google en el ámbito de las búsquedas en China. En cualquier caso, no es la primera vez que las autoridades chinas se lanzan al ataque creando una aplicación propia para impedir el uso en el país de herramientas de otros países. También se ha actuado así con la creación de redes sociales y sistemas de cartografía dependientes directamente del gobierno.

También el gobierno estaría reclutando cerca de 20.000 personas para desarrollar su propia Wikipedia, pero sin la participación del público. "El intento de compilar las 300.000 entradas que abarcan la ciencia, la literatura, la política y la historia está dirigido por el Departamento de Propaganda Central del partido comunista gobernante que guía la opinión pública a través de instrucciones a los medios de comunicación, a las empresas de Internet y a la industria editorial, así como a supervisar el sector de la educación. Ha instruido a la Encyclopedia of China Publishing House, conocida por haber editado la enciclopedia China, para producirlo"[270].

SUDAMÉRICA

República Federativa de Brasil

En 1996, la Política Nacional de Defensa[271] de Brasil,

> ...estaba orientada a las amenazas externas, y tenía como finalidad establecer los objetivos para la defensa de la Nación y, asimismo, servir como guía para la preparación y la utilización de la capacidad nacional, en todos los niveles y los ámbitos de poder, y con la participación de los sectores civil y militar.

En 2005 se publica una nueva Política Nacional de Defensa[272] en la cual se precisa que la seguridad, en líneas generales, "...es la condición en la que el estado, la sociedad o los individuos no se sienten expuestos a riesgos o amenazas, mientras que defensa es acción efectiva para lograrse o mantenerse el grado de seguridad deseado".

---

270 China has recruited 20000 people to create its own Wikipedia, but public can't edit it; Disponible en: http://economictimes.indiatimes.com/magazines/panache/china-has-recruited-20000-people-to-create-its-own-wikipedia-but-public-cant-edit-it/articleshow/58527116.cms

271 Libro Blanco de la Defensa de Brasil; Disponible en: http://www.oas.org/csh/spanish/doclibrdefBras.asp.

272 Política de Defensa Nacional de Brasil 2005; Disponible en:, http://www.oas.org/csh/spanish/doclibrdef.asp.

Finalmente, en 2012, la Política Nacional de Defensa[273] de la República Federativa de Brasil adopta los siguientes conceptos, ya existentes en el documento de 2005:

Seguridad: es la condición que permite al país la preservación de la soberanía y de la integridad territorial, la realización de sus intereses nacionales, libre de presiones y amenazas de cualquier naturaleza, y la garantía a los ciudadanos del ejercicio de los derechos y deberes constitucionales;
Defensa Nacional: es el conjunto de medidas y acciones del estado, con énfasis en el campo militar, para la defensa del territorio, la soberanía y los intereses nacionales contra amenazas preponderantemente externas, potenciales o manifiestas.

Sin embargo, debe notarse que las Fuerzas Armadas del Brasil, en la enmienda número 18 de 1998, establece que su misión constitucional, es la garantía de la ley y del orden.

> Art. 142. *As Forças Armadas, constituídas pela Marinha, pelo Exército e pela Aeronáutica, são instituições nacionais permanentes e regulares, organizadas com base na hierarquia e na disciplina, sob a autoridade suprema do Presidente da República, e destinam-se à defesa da Pátria, à garantia dos poderes constitucionais e, por iniciativa de qualquer destes, da lei e da ordem.*

En diciembre de 2008, la Estrategia Nacional de Defesa (END) estableció prioridades en tres sectores estratégicos para la Defensa Nacional: en el Nuclear, en el Cibernético y el Espacial. Como resultado de ello se constituyó el Sector Cibernético en el cual se distinguen dos campos de actuación: la Seguridad Cibernética, a cargo de la Presidencia de la República, y la Defensa Cibernética, a cargo del Ministerio de Defensa, por medio de las Fuerzas Armadas.
La *Diretriz* Ministerial nº 0014 de 2009 del *Ministerio de Defesa*, del 9 de noviembre de 2009, definió las normas para el cumplimento de la END en los sectores estratégicos de la defensa, estableciendo las responsabilidades para cada fuerza armada. Al ejército, le cupo la responsabilidad de la coordinación e integración del Sector Cibernético.

Para la Política Nacional de Defensa de Brasil de 2012[274]:

> La seguridad tradicionalmente fue vista sólo desde el ángulo de la confrontación entre las naciones, o sea la protección contra las amenazas de otras comunidades políticas o, más simplemente, como la defensa externa. A medida que las sociedades se desarrollaron y se profundizó la interdependencia entre los estados, se añadieron nuevas exigencias. Gradualmente, se amplió el concepto de seguridad y ahora abarca los campos político, militar, económico, científico-tecnológico, ambiental y otros. Pre-

273 Política nacional de defensa de Brasil, desde un servidor brasileño, idioma portugués Disponible en: http://www.defesa.gov.br/arquivos/2012/mes07/pnd.pdf.

274 Brasil, POLÍTICA NACIONAL DE DEFESA; Disponible en: http://www.infodefensa.com/wp-content/uploads/PoliticaNacionalDefensa_Brasil.pdf

servar la seguridad requiere de medidas de amplio espectro, que involucran, además de la defensa externa: la defensa civil, la seguridad pública y las políticas económicas, social, educativa, ambiental, de salud, científico tecnológica, industrial. En fin, de distintas acciones, muchas de las cuales no implican la participación de las fuerzas armadas. Cabe destacar que la seguridad puede ser abordada desde el individuo, la sociedad y el estado, desde donde surgirán definiciones con diferentes perspectivas.

En conclusión, Brasil, que en 1996 orientaba su Política de Defensa Nacional hacia las amenazas externas exclusivamente, según lo expresa la Política de Defensa Nacional 2005, desde ese entonces hasta la fecha adopta la recomendación de "Especialistas convocados por la Organización de las Naciones Unidas (ONU) en Tashkent, que, en el año 1990 definieron la seguridad como "una condición por la cual los estados consideran que no existe peligro de una agresión militar, presiones políticas o coerción económica, de manera que pueden dedicarse libremente a su propio desarrollo y progreso"[275]. Este concepto es similar al del documento ONU AG 40/553 de 1986 Conceptos de Seguridad mencionado en la nota 213 de la presente investigación[276].

En enero de 2015 se aprobó la Estrategia General de Tecnología de la Información y las Comunicaciones (EGTIC) que incluye como instrumento para su gestión el establecimiento de la Dirección de Tecnología de la Información y Comunicaciones (TIC)[277].

Asimismo, en mayo de 2015, el Gabinete de Seguridad del Gobierno de Brasil presenta la Estrategia de Seguridad de la Información y las Comunicaciones y de Seguridad Cibernética de la Administración Pública Federal 2015-2018 la cual constituye un minucioso detalle y mapeo estratégico de las diferentes atribuciones específicas de los órganos del estado del país responsables en la materia y describe los mecanismos disponibles para la participación de la sociedad (empresas, universidades y órganos de la comunidad) en la elaboración de políticas y acciones en materia de protección de infraestructuras críticas, evitando riesgos en el espacio cibernético y procurando incrementar el *know-how* industrial con especial énfasis en las empresas de defensa tendiente a la homologación de productos y servicios del sector[278].

República de Chile

El Gobierno de Sebastián Piñera (2010-2014) difundió en el mes de junio de 2012 la

275 Política Nacional de Defensa 2005, Decreto Nro. 5.484 del 30 de junio de 2005, punto 1. 3 [...] Especialistas convocados pela Organização das Nações Unidas (ONU) em Tashkent, no ano de 1990, definiram a segurança como "uma condição pela qual os Estados consideram que não existe perigo de uma agressão militar, pressões políticas ou coerção econômica, de maneira que podem dedicar-se livremente a seu próprio desenvolvimento e progresso"; Disponible en: https://www.planalto.gov.br/ccivil_03/_Ato2004-2006/2005/Decreto/D5484.htm

276 Esta investigación no ha encontrado referencia alguna a una supuesta reunión de especialistas convocados por la ONU en Tashkent en el año 1990, a la que alude este Decreto Presidencial de Brasil a pesar que diferentes trabajos y monografías, que se refieren a la seguridad, citan como fuente de tal reunión al emncionado decreto.

277 Brasil, Estrategia General de Tecnología de la Información y las Comunicaciones (EGTIC) 2015 Disponible en: http://www.sti.ufpb.br/documentos/EGTIC.pdf

278 Brasil, Gabinete de Seguridad, Estrategia de Seguridad de la Información y las Comunicaciones y de Seguridad Cibernética de la Administración Pública Federal 2015-2018; Disponible en: http://dsic.planalto.gov.br/documentos/publicacoes/4_Estrategia_de_SIC.pdf

primera Estrategia Nacional de Seguridad y Defensa, para luego publicar en el mes de agosto su versión corregida. Sin embargo, ambos documentos no fueron oficializados ni por su gobierno ni por la actual administración de la presidente Bachelet (2014-2018)[279].

En dicho documento [280]se buscaba orientar y coordinar la acción de distintos organismos e instituciones nacionales para enfrentar adecuadamente los desafíos de seguridad en el período 2012-2024.

Los criterios orientadores utilizados en la elaboración de la estrategia fueron cinco, a saber: 1) La protección de las personas como eje, 2) La correlación entre seguridad y desarrollo, 3) La complementariedad entre seguridad y defensa, 4) La cooperación internacional como imperativo nacional, y 5) La seguridad como política pública.

De acuerdo al texto, dichos criterios reflejarían el concepto de "seguridad ampliada", adoptado como enfoque para la elaboración de la estrategia. A grandes rasgos, este concepto se traduce en una mirada integral de los desafíos de seguridad de diversa naturaleza –en su mayoría de carácter transnacional-, para buscar fórmulas de coordinación que permitan el uso eficaz y eficiente de los medios y recursos.

En lo que respecta a la ciberseguridad y a la ciberdefensa, si bien la República de Chile aún no posee una normativa como la de Brasil, dos hechos importantes han ocurrido en 2015.

Por un lado, el 10 de abril de 2015 se creó el Comité Interministerial de Ciberseguridad (CIC), del que participaron, entre otros, el Ministerio del Interior, el Ministerio de Justicia, el Ministerio de Relaciones Exteriores y el Ministerio de Defensa.

Por otro lado, en el marco del Seminario Internacional sobre Ciberseguridad y Ciberdefensa, organizado por el Centro de Estudios Informáticos de la Facultad de Derecho de la Universidad de Chile, el subsecretario de Relaciones Exteriores, Edgardo Riveros anunció que el gobierno chileno estaba trabajando en la creación de la Política Nacional de Ciberseguridad la cual sería presentada al país en marzo de 2016[281].

Riveros agregó que

> ...los temas sobre Ciberseguridad y Ciberdefensa son extraordinariamente relevantes en la agenda global y, por ende, importantes para el país, porque los desafíos y amenazas que se pueden enfrentar en el espacio cibernético, que no conocen fronteras, son cada día más complejos y difíciles de predecir.

Finalmente, el 27 de abril de 2017, la presidenta Michelle Bachelet Jeria presentó la

279 Chile, Estrategia Nacional de Seguridad y Defensa Nacional; Disponible en: el sitio de la Academia Nacional de Estudios Políticos y Estratégicos ANEPE http://esd.anepe.cl/wp-content/uploads/2015/04/ESD04ART05.pdf.

280 Biblioteca del Congreso Nacional de Chile, La Estrategia de Seguridad y Defensa de Chile, Síntesis y opiniones; Disponible en: www.bcn.cl/obtienearchivo?id=repositorio/10221/15344/1/...v6.

281 Troncoso Javier, artículo en el blog Oh MyGeek, 27 noviembre 2015 Disponible en: http://www.ohmygeek.net/2015/11/27/chile-politica-nacional-ciberseguridad/

"Política Nacional de Ciberseguridad[282] (PNCS) 2017-2022 para las ciberseguridades "una condición caracterizada por un mínimo de riesgos para el ciberespacio, entendido como el conjunto de infraestructuras físicas, lógicas y las interacciones humanas que allí ocurren. En este conjunto, y siguiendo estándares internacionales, los atributos clave a proteger son la confidencialidad, integridad y disponibilidad de la información, los que a su vez generan un ciberespacio robusto y resiliente".

Esta política fue elaborada por el Comité Interministerial sobre Ciberseguridad, integrado por las Subsecretarías de Interior, Relaciones Exteriores, Defensa, Hacienda, Secretaría General de la Presidencia, Economía, Justicia, Telecomunicaciones y la Agencia Nacional de Inteligencia siendo su Secretario Ejecutivo, el Subsecretario de Defensa Marcos Robledo Hoecker.

En lo que respecta a la ciberdefensa, la PNCS dispone que[283]:

> Dado que las redes y sistemas de información de la Defensa Nacional constituyen una infraestructura crítica para la seguridad exterior y el ejercicio de la soberanía del país, y a las atribuciones constitucionales y legales de la Defensa Nacional, el Ministerio de Defensa, durante el año 2017 preparará y publicará políticas específicas de ciberdefensa, que contemplen las definiciones políticas en torno a cómo serán protegidas estas redes, y cómo las capacidades de la Defensa Nacional pueden colaborar en la formación de un ciberespacio libre, abierto, seguro y resiliente para el país.

Para la PNCS, uno de los objetivos de alto nivel es la relación con la cooperación y relaciones internacionales en torno a la ciberseguridad en el contexto global y, para ello, la contempla una medida específica vinculada con la elaboración de una estrategia en estas materias por parte del Ministerio de Relaciones Exteriores.

En cuanto a las fuerzas armadas, la PNCS establece que "Las instituciones de las Fuerzas Armadas están a cargo de proteger su propia infraestructura de la información, además de colaborar en las tareas de ciberseguridad que correspondan en relación con la seguridad nacional y el sistema nacional de inteligencia".

República Argentina

En la República Argentina, el "Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad" (ICIC), creado mediante la Resolución JGM Nº 580/2011, que se mantiene en vigencia al momento en que se realiza este trabajo, tiene como finalidad

> ...impulsar la creación y adopción de un marco regulatorio específico que propicie la identificación y protección de las infraestructuras estratégicas y críticas del

282 Gobierno de Chile, Política Nacional de Ciberseguridad de Chile; Disponible en: http://ciberseguridad.interior.gob.cl/media/2017/05/PNCS-CHILE-FEA.pdf

283 Ibidem. P. 15

Sector Público Nacional, los organismos inter jurisdiccionales y las organizaciones civiles y del sector privado que así lo requieran, y la colaboración de los mencionados sectores con miras al desarrollo de estrategias y estructuras adecuadas para un accionar coordinado hacia la implementación de las pertinentes tecnologías, entre otras acciones.[284]

La Directiva de Política de Defensa Nacional 2014, mantuvo lo establecido en la anterior PNDN de noviembre de 2009 y ordenó que el Ministerio de Defensa adhiriese al "Programa Nacional de Infraestructuras Críticas de la Información y Ciberseguridad" de la Oficina Nacional de Tecnologías de la Información (ONTI) de la Jefatura de Gabinete de Ministros.

Por Decisión Administrativa 15/2015 del Jefe de Gabinete de Ministros se creó la Dirección General de Ciberdefensa en el ámbito del Ministerio de Defensa y se le asignó la responsabilidad de:

- Asistir en el planeamiento, diseño y elaboración de la política de ciberdefensa de acuerdo a lo establecido en el Ciclo de Planeamiento de la Defensa Nacional en coordinación con la Subsecretaría de Planeamiento Estratégico y Política Militar.
- Entender en la coordinación con los organismos y autoridades de los distintos poderes del Estado para contribuir desde la Jurisdicción a la política nacional de ciberseguridad y de protección de infraestructura crítica.
- Intervenir en la orientación, dirección y supervisión de las acciones en materia de ciberdefensa ejecutadas por el Nivel Estratégico Militar.
- Ejercer el control funcional sobre el Comando Conjunto de Ciberdefensa de las Fuerzas Armadas.
- Intervenir en la evaluación y aprobación de los planes militares de desarrollo de capacidades de ciberdefensa, en la doctrina básica y en las publicaciones militares pertinentes, cualquiera sea su naturaleza.
- Intervenir en el diseño de políticas, normas y procedimientos destinados a garantizar la seguridad de la información y a coordinar e integrar los centros de respuesta ante emergencias teleinformáticas.
- Fomentar políticas de convocatoria, captación, incentivo y formación de recursos humanos para la ciberdefensa para mantener un plantel adecuado.
- Promover vínculos sistemáticos de intercambio y cooperación en materia de ciberdefensa con los ámbitos académico, científico y empresarial.
- Impulsar acuerdos de cooperación e intercambio en materia de investigación y asistencia técnica en ciberdefensa con organismos públicos y privados.
- Asistir en el desarrollo doctrinario, en el diseño y fortalecimiento de capacidades y en la elaboración de la estrategia de ciberdefensa de conformidad con los lineamientos del Ciclo de Planeamiento de la Defensa Nacional.

284 Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad; Disponible en: http://www.icic.gob.ar/

Por Decreto 13/2016[285] se creó, dentro del Ministerio de Modernización, la Subsecretaría de Tecnología y Ciberseguridad, cuyos objetivos, entre otros son los de:

- Entender en la elaboración de la estrategia nacional de Infraestructura tecnológica, la protección de infraestructuras críticas de información y ciberseguridad, en el ámbito del Sector Público Nacional.
- Entender en la administración, supervisión y operación de los sistemas informáticos del Sector Público Nacional, garantizando la disponibilidad y confiabilidad de los mismos.
- Entender en materia de dictado de normas, políticas, estándares y procedimientos de Tecnología y Seguridad Informática en el ámbito de su competencia.
- Entender en los procesos relativos al accionar del equipo de respuesta a emergencias informáticas a nivel nacional (CERT NACIONAL).[286]
- Difundir las mejores prácticas y elaborar políticas de capacitación para el Sector Público Nacional y contribuir a la capacitación de las organizaciones civiles, del sector privado y del ámbito académico en temas de seguridad de la información y protección de información crítica, que así lo requieran.
- Dirigir y supervisar el accionar de la Oficina Nacional de Tecnologías de la Información (ONTI)

Por Decreto 226/2016 se la elevó al rango de subsecretaría, dependiente de la Secretaría de Ciencia, Tecnología y Producción para la Defensa del Ministerio de Defensa. Esta Subsecretaría tiene dos direcciones: la Dirección Nacional para el Desarrollo Científico de la Ciberdefensa y la Dirección Nacional de Diseño de Políticas de Ciberdefensa.

En el marco de la visita del presidente Macri a los Estados Unidos, en abril de 2017, "la Casa Blanca y el Gobierno argentino anunciaron que trabajarán juntos en materia de ciberseguridad para lo cual, se conformará un "Grupo de Trabajo Intergubernamental Bilateral sobre Política Cibernética" para la identificación de preocupaciones cibernéticas de interés mutuo y el desarrollo de iniciativas conjuntas"[287].

Además, ambos países se comprometieron a fortalecer la colaboración en el marco de los foros internacionales pertinentes y prevén incrementar la cooperación en las siguientes áreas: ciberseguridad; defensa cibernética; seguridad internacional en el ciberespacio; y respuestas de índole legal a los delitos cibernéticos.

El 28 de julio de 2017, mediante el decreto 577/2017, el Gobierno nacional creó el Comité de Ciberseguridad con el objetivo de desarrollar una estrate gia nacional de ciber-

---

285 República Argentina. Decreto 13/2016 Decreto N° 357/2002. Modificación. Bs. As., 05/01/2016 Disponible en: http://servicios.infoleg.gob.ar/infolegInternet/anexos/255000-259999/257556/norma.htm

286 En Sudamérica hay 14 países con Equipos de Respuesta a Incidentes de Seguridad Cibernética (CSIRT), entre los que se encuentran el ArCERT (Argentina, 1999, que posteriormente daría lugar al ICIC), el CICERT (Chile, 2001), el CTIR-GOV (Brasil, 2004), el CTIRGT (Guatemala, 2006), el CERTUy (Uruguay, 2008), el VenCERT (Venezuela, 2008), el PerCERT (Perú, 2009) y el ColCERT (Colombia, 2011).

287 Argentina. Gob.ar, Argentina y Estados Unidos trabajarán juntos en materia de Ciberseguridad; Disponible en: https://www.argentina.gob.ar/noticias/argentina-y-estados-unidos-trabajaran-juntos-en-materia-de-ciberseguridad

seguridad que proteja el ciberespacio, que tenga la capacidad de responder a incidentes de gran escala y sugiera una legislación en la materia[288].

El documento señala entre sus fundamentos la necesidad en materia de ciberseguridad de atender "diversos aspectos como proteger las infraestructuras críticas y poseer la capacidad para colaborar con otros países". La norma señala que la elaboración de una estrategia deberá realizarse en coordinación con las áreas competentes de la Administración Pública Nacional e impulsar el dictado de un marco normativo en la materia.

En los considerandos del decreto se afirma que encarar una adecuada protección en materia de ciberseguridad "es una tarea compleja que resulta necesaria en la actualidad, debido al incremento exponencial y a la diversidad de las amenazas y ataques informáticos".

Conclusiones del capítulo

Los acontecimientos ocurridos durante los últimos años, desde los ataques del 11 de septiembre de 2001 a los recientes actos de ciberespionaje, realizados por los estados o por espías corporativos con fines de lucro o de mejora estratégica, utilizando técnicas cada día más avanzadas; pasando por las amenazas de *Anonymous, Wikileaks* y los efectos de malware como Stuxnet, han llevado a la mayoría de los gobiernos a incluir en sus agendas el desarrollo de estrategias nacionales de ciberseguridad y de ciberdefensa, de las cuales se derivan las doctrinas militares en el campo de la ciberdefensa.

Tanto los estados europeos analizados como la República de Brasil y Colombia se han organizado a partir de una Estrategia Nacional de Defensa y Seguridad, en la cual se definen determinadas maniobras para enfrentar las amenazas y los riesgos que ellas implican. La República de Chile lo ha hecho a partir de la Política Nacional de Ciberseguridad.

Dichas estrategias dan lugar a las distintas facetas o aspectos como son la defensa económica, la defensa territorial, la defensa aérea, la defensa de las fronteras, y dado que el espacio cibernético es un ambiente más, también para él se considera que debe existir una ciberdefensa que garantice la ciberseguridad y se inserte en una Estrategia de Seguridad Nacional.

En ellas, los países dejan reflejados los riesgos y amenazas que son necesarios encarar en un mundo continuamente cambiante y, por lo general, adoptan el concepto de seguridad del Estado, en los términos establecidos por la Asamblea General de la Organización de las Naciones Unidas en su Documento A 40/553 del año 1986, es decir, como "la condición en que los estados pueden libremente continuar con su desarrollo y progreso, al no existir peligro de un ataque militar, presión política o coerción económica".

En estas estrategias de seguridad y defensa se determinan objetivos, líneas o cursos de acción como así también normas y directivas para proteger las TIC[289] y se obliga a los distintos usuarios, estatales o privados, a informar ataques o intrusiones cibernéticas.

---

288 Disponible en: http://servicios.infoleg.gob.ar/infolegInternet/anexos/275000-279999/277518/norma.htm

289 Entiéndase dicho acrónimo como el conjunto de recursos necesarios para manipular la información: las computadoras, los programas informáticos y las redes necesarias para convertirla, almacenarla, administrarla, transmitirla y encontrarla.

Tales normativas habitualmente contemplan la asignación de los recursos adecuados; definen públicamente lo que entienden por ciberseguridad y ciberdefensa y explicitan aquellas actividades que podrían ser consideradas como una agresión y, por ende, ser respondidas con actos de defensa propia; crean mecanismos bilaterales o multilaterales de cooperación para compartir información sobre las amenazas cibernéticas y sobre las técnicas que pueden utilizarse para mitigarlas. Además, desarrollan ejercicios y adiestramientos realistas.

Sin embargo, todas esas iniciativas no han logrado resolver el problema de la seguridad y la defensa. Paradójicamente, la cooperación entre las distintas agencias del gobierno, las compañías privadas y el público para combatir las ciberamenazas es mucho más complicada de lo que debiera ser. Nadie quiere aparecer como víctima de un ciber ataque para no ser tildado de incauto y/o para no alertar al hacker o al atacante. En especial, esto pasa con las entidades bancarias que no revelan intrusiones cibernéticas en sus sistemas para no ahuyentar potenciales clientes.

También, se puede apreciar que la mayoría de las estrategias reconocen que la seguridad de los sistemas de información que comprenden la Internet requiere de una alianza entre el gobierno, las universidades y la industria. La sociedad política y la sociedad civil deben unificar esfuerzos.

Esta integración estatal se encuentra ya instrumentada en muchos países, y el caso comparado entre la defensa cibernética de Estados Unidos y Brasil está estudiado en profundidad en el libro Gestión de Inteligencia en las Américas de la Universidad Nacional de Inteligencia de Washington DC.

En la Argentina hasta el momento, a diferencia de otros países, no existe una Política o Estrategia Nacional de Defensa Cibernética, como tampoco una Estrategia Nacional de Seguridad Cibernética ni una Estrategia Nacional de Seguridad. El decreto 577/2017 es un paso importante para su concreción.

La Política o Estrategia Nacional de Defensa Cibernética debería contener el objeto de la Ciberdefensa en las Fuerzas Armadas, los objetivos estratégicos, y las directrices o líneas de acción para cada uno de ellos.

A modo de ejemplo, en los anexos, en forma de tabla se muestran dos modelos de posibles objetivos estratégicos y el detalle de las directrices o líneas de acción para cada uno de ellos, que podrían ser perfeccionados y servir como base para elaborar dicho documento. Estos objetivos no son excluyentes, sino que podrían complementarse.

Debe quedar claro que estas estrategias reconocen el derecho de los privados a tener su propia seguridad informática, pero establecen normas para que todos contribuyan a alcanzar la seguridad cibernética del país.

En el siguiente capítulo podrá verse cómo determinados países han desarrollado sus doctrinas o directivas de defensa cibernética a partir de políticas de ciberseguridad y ciberdefensa nacionales.

CAPÍTULO 3

DOCTRINAS MILITARES EN EL CAMPO DE LA CIBERDEFENSA Y LA CIBERSEGURIDAD

Introducción

El Día de los Inocentes de 1995 (28 de diciembre), la casa de un joven fue allanada por la justicia argentina, luego de que el Gobierno de Estados Unidos alertara sobre reiteradas intrusiones a varias de sus redes informáticas de Defensa, entre ellas la del Pentágono. Utilizando las líneas 0800 de uso gratuito de Telecom, Ardita[290], así era el apellido del intruso, logró acceder al sistema de redes de la Universidad de Harvard y desde allí, a información sobre el diseño de radares y aviones militares[291].

Veintidós años más tarde, el 12 de mayo de 2017 [292]

El mundo se asomó al apocalipsis cibernético. Un ataque masivo e indiscriminado con un virus informático afectó a empresas de servicios, bancos e instituciones públicas en por lo menos 74 países y desató una alerta de seguridad de una dimensión pocas veces vista. El golpe causó especial impacto en España, donde infectó computadoras de la sede central de Telefónica, y en Gran Bretaña, donde provocó un colapso en el Servicio Nacional de Salud (NHS, por sus siglas en inglés). En Estados Unidos alcanzó a la empresa FedEx. Rusia, China, Japón, Portugal, Italia, Egipto, Filipinas y Turquía sufrieron también complicaciones considerables. Los hackers que desata-

290 Después de soportar dos procesos, uno en la Argentina y otro en los Estados Unidos -de los que quedó absuelto-, Ardita fundó Cybseg, una empresa de seguridad informática con presencia en varios países de América latina.

291 Diario La Nación, Cabot, Diego, "Ardita, de temido hacker a experto en seguridad informática" jueves 02 de diciembre de 2004; Disponible en: http://www.lanacion.com.ar/659203-ardita-de-temido-hacker-a-experto-en-seguridad-informatica

292 Diario La Nación, Rodríguez Yebra, Martín, Alarma en más de 70 países por un ciberataque masivo de alto impacto, Edición impresa página 1; Disponible en: http://www.lanacion.com.ar/2023417-alarma-en-mas-de-70-paises-por-un-ciberataque-masivo-de-alto-impacto

ron la ola global de ciberataques usaron herramientas robadas a la Agencia de Seguridad Nacional de Estados Unidos (NSA) para aumentar el poder de daño de un software malicioso conocido como WannaCry, según analistas.

Según el portal del diario El País de España[293],

Debido a ese ataque, la empresa Renault debió suspender la producción en varias plantas, una decena de grandes empresas españolas de servicios sufrieron el ciberataque. La compañía más afectada fue Telefónica. En el Reino Unido afectó simultáneamente a ordenadores y teléfonos de 16 hospitales y centros de salud de Londres, Nottingham, Herefordshire, Blackburn y Cumbria, según el servicio nacional de salud (NHS). El Banco Central de Rusia indicó que varias entidades financieras habían sufrido el ataque. Fedex admitió haber sufrido "interferencias" en algunos de sus equipos que funcionan con el sistema operativo Windows a consecuencia de "un *malware*". Un usuario de la red social Reddit que se ha identificado como trabajador de la compañía escribió: "Todos los sistemas se han visto afectados en el servidor principal de Memphis, se cayeron un montón de importantes cintas que usamos para mover la carga entre los centros pequeños y los aviones

En China, varias escuelas y universidades fueron también víctimas del ataque, según informó la agencia oficial Xinhua. Los medios estatales no especificaron qué centros se han visto afectados, aunque hablan de "docenas". El ciberataque afectó el sistema informático de la compañía de trenes alemana, Deutsche Bahn (DB), aunque no alteró el tráfico ferroviario. El Tribunal de Justicia brasileño confirmó que algunos equipos de la institución sí estaban afectados. Entre las instituciones afectadas figura, según el diario *El Tiempo,* el Instituto Nacional de Salud. Este organismo suspendió la actividad de su página web hasta la próxima semana. En Colombia, el servicio más perjudicado fue el de trasplantes porque el Instituto Nacional de Salud es quien administra los turnos para ese tipo de intervención quirúrgica. También lo fue el Ministerio de Justicia, cuya web seguía sin funcionar al día siguiente del ataque.

Durante las últimas décadas, los avances tecnológicos han transformado las comunicaciones y la capacidad de adquirir, difundir y utilizar información en una gama de ambientes operacionales. Como resultado, los ejércitos modernos mejoraron sus capacidades de mando y control mediante el uso de la información a través de la guerra centrada en redes. La convergencia creciente de las operaciones militares y comerciales amerita tener en cuenta la posibilidad de que la comunicación y las infraestructuras de información sean componentes viables, tanto objetivos como armas, en tiempos de guerra.

El progreso en los últimos años indica que Internet y la tecnología de la comunicación en particular se están convirtiendo en un teatro factible de futuros conflictos mili-

293 El ataque alcanza ya a un centenar de países: desde Renault en Francia hasta bancos rusos; 13 de mayo de 2017; Disponible en: http://tecnologia.elpais.com/tecnologia/2017/05/13/actualidad/1494668788_755982.html

tares generalizados en el espacio cibernético. Esto ha provocado una notable evolución de las capacidades militares relacionadas con la guerra cibernética. En este contexto, y como se verá en este capítulo, algunos estados se están preparando para ser el blanco de un ciberataque de guerra y están dispuestos a lanzar una contraofensiva. De aquí que ya han comenzado los preparativos para este tipo de conflictos en varios países, entre los que se incluye Israel, Corea del Norte, Irán y Rusia.

Cuando se examinan estas actividades desde una perspectiva más holística, la preparación de ambas capacidades ofensivas y defensivas tiene componentes técnicos y de políticas públicas.

En otras palabras, las naciones necesitan encontrar respuestas y soluciones debido a que las bombas son guiadas por satélites GPS; los drones son piloteados remotamente desde cualquier parte del mundo; los aviones de combate y buques de guerra son grandes centros de procesamiento de datos; e incluso el soldado de a pie está interconectado.

También, se puede hacer explotar gasoductos[294] y atacar refinerías de petróleo[295]; colapsar sistemas de control del tráfico aéreo; descarrilar trenes y subterráneos; modificar datos financieros; hacer caer la red eléctrica en el este de Estados Unidos[296]; o hacer que satélites giren fuera de control o en órbitas no planificadas.

La creciente conectividad a una Internet insegura multiplica las vías para los ataques cibernéticos; y la creciente dependencia de las computadoras aumenta el daño que pueden causar. Lo peor de todo es que la identidad del atacante puede seguir siendo un misterio.

Asimismo, se puede eliminar o cambiar el contenido de páginas web, dar órdenes falsas a fuerzas convencionales, interferir con el comando y control llevado a cabo con medios cibernéticos, bloquear o transferir fondos bancarios, borrar lecturas de controles de tránsito aéreo, e infinidad de tareas dedicadas a denegar el servicio en servidores, anular funcionamiento de sistemas completos de información y control, o saturar las redes con informaciones falsas. Además, y entre otras tantísimas cosas, se pueden abrir y cerrar compuertas de diques a voluntad, modificar la estructura de funcionamiento de molinos generadores eólicos, y cualquier otra actividad cuyos componentes se manejen con una IP.

Al solo efecto de alertar sobre las capacidades cibernéticas inesperadas, y a modo de ejemplo didáctico y simple de comprender para visualizar la gravedad del problema, se puedo imaginar lo siguiente: una persona compra un promocionado sistema de vigilan-

294 Durante la guerra fría, en junio de 1982, un satélite de alerta temprana estadounidense detectó una gran explosión en Siberia. ¿Un misil había sido lanzado? ¿Un ensayo nuclear? Era, al parecer, una explosión en un gasoducto soviético. La causa fue una falla en el sistema de control de computadoras que espías soviéticos habían robado de una empresa en Canadá. Lo que desconocían era que la CIA había manipulado el software para que " después de un prudente intervalo de tiempo, las velocidades de las bombas y los ajustes de las válvulas se volviesen a graduar y generasen presiones más allá de las aceptables para las tuberías, empalmes y soldaduras," según las memorias de Thomas Reed, un antiguo secretario de la Fuerza Aérea anterior. El resultado, dijo, "fue la explosión no nuclear más monumental y un incendio nunca visto desde el espacio". The Economist. Jul 1st 2010, Ataque de la CIA a un gasoducto en Siberia; Disponible en: http://www.economist.com/node/16478792

295 The New York Times. OCT. 23, 2012 Un virus borró los datos de tres cuartas partes de las computadoras de la corporación Aramco, reemplazándolos por una imagen de una bandera americana prendiéndose fuego; Disponible en: http://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html?_r=0

296 INQUISITR. News Worth Sharing. Cyber Attack by China on power grid alleged. January 17, 2014; Disponible en: http://www.inquisitr.com/1099181/cyber-attack-by-china-on-power-grid-alleged/

cia con cámaras, para el interior de su domicilio, que puede monitorear con su teléfono móvil a distancia. Para poder hacerlo, debe tener allí un dispositivo con una IP, que tendrá un usuario y una *password*. Normalmente, por *default* el usuario del dispositivo con IP es *admin* y la *password*, *admin*. Si la persona no tomó el cuidado de cambiar el usuario y la password, aquel que le instaló el sistema o cualquier otra persona bien podría tener acceso a lo que ocurre en el interior de su casa. Existen varios casos de robos en domicilios con este tipo de vigilancia, ya que los ladrones sabrán cuándo no hay nadie en la vivienda. Para interpretar la gravedad y el peligro que ello puede acarrear para la vida de los militares, habría que imaginar si esto ocurriera dentro de una instalación militar.

Es por ello que el objetivo de este capítulo se enfoca en los aspectos que tuvieron en cuenta países como Francia, Brasil, España y Estados Unidos, a partir de una Política o Estrategia Nacional de Defensa Cibernética para desarrollar una doctrina militar conjunta de ciberdefensa.

República de Francia

En Francia, en coherencia con la asignación de la función de la Autoridad Nacional de Defensa de los Sistemas de Información (ANSSI), la conducción de la defensa de los sistemas de información y comunicación del Ministerio de Defensa y los específicos de las fuerzas armadas es responsabilidad del Jefe del Estado Mayor Conjunto (EMA).

En el Ministerio de Defensa, esta protección, que toma el nombre de Lucha Defensiva Informática (LID), es proporcionada por las funciones de vigilancia, alerta y respuesta a las vulnerabilidades, amenazas e incidentes a través de la *Organisation permanente de veille, alerte et réponse* (OPVAR), la cual también es responsable de la administración de los planes Vigipirate y Piranet descriptos en el capítulo anterior.

En 2011, el gobierno francés dispuso la creación del cargo de Oficial General de la Ciberdefensa como encargado de coordinar las acciones del ámbito de la Defensa, el cual sirve de interfaz principal en caso de producirse una crisis cibernética.

Ese mismo año, fue promulgada la publicación *Concept interarmées (CIA)* 6.3 titulada *Cyberdéfense (CYBERDEF)*[297] que servirá de base para la elaboración de la doctrina de Ciberdefensa. En ella,

> ...se define en primer lugar, el marco general en que el Ministerio de Defensa es llamado a operar en el espacio cibernético. Luego analiza los fundamentos y principios que afectan a una eficaz defensa cibernética antes de deducir las capacidades que requiere: conocer el espacio cibernético y sus amenazas, anticipar posibles ciberataques, supervisar y evaluar la situación, el orden, proteger, investigar y defender, restaurar los sistemas, desarrollar las capacidades necesarias para estas acciones y finalmente inscribirse en cyber-resiliencia en el enfoque global de la resiliencia de la nación.

297 Centre interarmées de concepts, de doctrines et d'expérimentations (CICDE), Promulgation du Concept interarmées (CIA) 6.3 intitulé Cyberdéfense (CYBERDEF); Disponible en: http://www.cicde.defense.gouv.fr/spip.php?article968.

Dicha publicación fue derogada y reemplazada por la DIA – 3.40 *Cyberdeféns*e, que no se encuentra disponible en Internet.[298]

No obstante, del análisis de la publicación *"Doctrine d'emploi des forces"*[299] se puede apreciar que uno de los cinco esfuerzos que persigue el concepto de empleo de fuerzas es el de integrar las acciones de ciberdefensa a las operaciones militares.

Si bien Francia mantiene en reserva gran parte de sus documentos relacionados con la ciberdefensa, el contraalmirante Arnaud de Coustillière, responsable de la ciberdefensa indicó a fines de septiembre de 2014 que: "si podemos neutralizar los radares con el arma informática antes que, con un misil, es mucho mejor" ... "un ataque catastrófico contra las infraestructuras vitales sí puede producirse" ... "nos dirigimos hacia una militarización reforzada del espacio cibernético con un riesgo certero de engranaje donde los cibernautas (simples usuarios) serán las principales víctimas"[300].

De la información extraída de distintas fuentes públicas, puede decirse que, para hacer frente a los riesgos y amenazas que afectan los sistemas de información esenciales para el funcionamiento de la defensa y de las misiones que deben cumplir las fuerzas armadas, Francia posee una organización de ciberdefensa en la cual intervienen distintos actores[301].

Por un lado, existe una cadena de comando de operaciones conjuntas, bajo la autoridad del Jefe de Estado Mayor Conjunto, comandada por un General, dentro de la cual se encuentra el Centro de Planificación y Conducción de las Operaciones (CPCO). Como parte de sus atribuciones, cumple una doble función: sus responsabilidades son las operaciones en el CPCO, para la planificación, coordinación y el desarrollo de las operaciones de defensa del Ministerio y de los sistemas de información de las fuerzas armadas y, transversalmente, impulsar y coordinar el trabajo relativo a la ciberdefensa en el seno de las tres fuerzas armadas.

Para una respuesta rápida en caso de amenaza, el Centro de Análisis de Lucha Informática Defensiva (CALID, por sus siglas en francés) es el brazo ejecutor del Ministerio de Defensa. En colaboración con otras entidades ministeriales a cargo de la seguridad informática, participa permanentemente en la protección de los sistemas de información, monitorea las redes del Ministerio, detecta anomalías que ponen en peligro los sistemas de información y actúa en consecuencia.

En cuanto a la parte técnica de Ciberdefensa, la Dirección General del Armamento (DGA) división "seguridad de sistemas de información" (DGA-Il DGA - MI), en colaboración con la industria, promueve la innovación y el desarrollo de nuevas soluciones técnicas y profundiza la investigación sobre cinco ejes: criptografía, métodos formales, se-

---

298 Información Disponible en: http://www.cicde.defense.gouv.fr/spip.php?rubrique50

299 Centre interarmées de concepts, de doctrines et d'expérimentations, Doctrine d'emploi des forces, Doctrine interarmées, DIA-01(A)_DEF (2014), N° 128/DEF/CICDE/NP du 12 juin 2014; Disponible en: http://www.cicde.defense.gouv.fr/IMG/pdf/20140612_np_cicde_dia-01-def.pdf

300 Febbro Eduardo, Rusia y Occidente aceleran su guerra cibernética, Página 12, 28 septiembre 2014; Disponible en: http://www.pagina12.com.ar/diario/elmundo/4-256329-2014-09-28.html .

301 Información extraída de la página web del Ministerio de Defensa de Francia; Disponible en: http://www.defense.gouv.fr/portail-defense/enjeux2/la-cyberdefense/la-cyberdefense/organisation

guridad de sistemas de explotación y de redes, seguridad electrónica y software, y análisis y manipulación de códigos de software.

En el nivel interagencial contribuyen a la protección de los sistemas de información, la Agencia Nacional de Seguridad de los Sistemas de Información (ANSSI), dependiente del Secretario General de Defensa y Seguridad nacional (SGDSN), bajo la autoridad del Primer Ministro, como así también el Ministerio del Interior, el Ministerio de Relaciones Exteriores, los denominados Operadores de Vital Importancia (OIV) relacionados con la defensa, y los fabricantes de sistemas de información de defensa.

Sin embargo, y pese a todas estas precauciones técnicas, en 2008, un hombre, cuyo nombre no se ha hecho público, se hallaba desempleado y trataba de ahorrar dinero en llamadas telefónicas usando Skype. Por ello, accedió a Internet en busca de códigos numéricos que le permitieran no pagar las llamadas a teléfonos fijos por medio de esta aplicación informática. Probando uno de los consejos recibidos en un foro, empezó a marcar números al azar para conectarse con alguien.

En algún momento le respondió el Departamento de Deudas del Banco de Francia, aunque él no fue consciente de ello, ya que la voz automática que le contestó no se identificó, sino que le pidió marcar seis cifras. Sin pensarlo mucho, marcó los números del uno al seis en orden ascendente. No sucedió nada más y el hombre colgó. Al otro lado del teléfono, sin embargo, la llamada tuvo unas consecuencias totalmente imprevistas: el servicio del banco quedó inutilizado por dos días.

Encontrar al "pirata informático" accidental no debería haber sido complicado, ya que había usado su verdadero nombre y dirección para entrar en Skype. No obstante, la Policía tardó dos años en localizarlo. Luego de ello, comenzó un proceso penal contra él por acusaciones de piratería informática. "Al parecer, los representantes de las fuerzas del orden quedaron asombrados tras descubrir que el supuesto hacker había tumbado el sistema de seguridad del principal banco del país sin ninguna intención de hacerlo y con ayuda de un ordenador anticuado y barato"[302].

Otros países de la Unión Europea

Para Carmen Cristina Cîrlig [303]

> En la Unión Europea hay distintas prácticas nacionales sobre ciberdefensa entre los estados miembro. Casi todos han adoptado una estrategia de seguridad cibernética nacional, o mencionado la seguridad cibernética como un aspecto importante de sus estrategias de seguridad nacional o han creado estructuras para hacer frente a las amenazas cibernéticas. Cerca de quince estados miembros han incluido una pers-

302 RT Noticias, Hackearon el Banco de Francia, noticia del 23 septiembre 2012; Disponible en: https://actualidad.rt.com/actualidad/view/54355-sabe-contar-seis-puede-hackear-sistema-banco-francia

303 Cîrlig, Carmen Cristina; Cyber defence in the EU Preparing for cyber warfare? European Parliamentary Research Service; Disponible en: http://www.europarl.europa.eu/EPRS/EPRS-Briefing-542143-Cyber-defence-in-the-EU-FINAL.pdf

pectiva militar de defensa cibernética en sus enfoques nacionales, pero muy pocos admiten haber invertido en armas cibernéticas.

Según la autora:

- **Dinamarca:** sobre la base del Acuerdo de Defensa para 2013-2017 estableció un Centro de Ciberseguridad dependiente del Ministerio de Defensa y decidió fortalecer las capacidades militares a través de una capacidad de operaciones de red de computadoras para estar en condiciones de ejecutar operaciones militares defensivas y ofensivas en el ciberespacio;
- **Finlandia:** anunció en 2011 que iba a invertir en el desarrollo de armas de la ciberdefensa. Su Estrategia de Seguridad Cibernética Nacional 2013 estableció que las Fuerzas finlandesas "crearán una capacidad integral de ciberdefensa", que incluirá la inteligencia cibernética, la guerra cibernética y capacidades de protección. Una unidad de defensa cibernética en guerra cibernética debía estar en condiciones de operar en 2015;
- **Italia:** ha establecido una unidad de guerra electrónica militar responsable de la inteligencia, vigilancia, adquisición de blancos y reconocimiento. Su Marco Estratégico Nacional para Seguridad del Ciberespacio de 2013, el Plan Nacional de ciberprotección y seguridad de la información y las directrices de defensa en el ciberespacio forman el marco de la política de ciberseguridad y ciberdefensa. Ellas señalan la necesidad de desarrollar las capacidades de inteligencia cibernética y ciberdefensa y las estructuras de comando y control "para planear y dirigir las operaciones militares en el ciberespacio".
- **Países Bajos:** adoptaron una estrategia de defensa cibernética en 2012 en la cual se establecen seis prioridades: la adopción de un enfoque integral; el fortalecimiento de las capacidades de la ciberdefensa; el desarrollo de capacidades militares cibernéticas ofensivas; el fortalecimiento de capacidades de inteligencia en el ciberespacio; el fomento, la innovación y la contratación de personal calificado; y la intensificación de la cooperación a nivel nacional e internacional. Un comando de ciberdefensa conjunto, creado en septiembre de 2014, dentro del ejército holandés, es el responsable del desarrollo de las capacidades cibernéticas.
- La Estrategia de ciberseguridad del **Reino Unido** de 2011 caracteriza a los ataques cibernéticos como una amenaza para la seguridad nacional y tiene como objetivo, entre otras cosas, la defensa de la infraestructura nacional contra ataques cibernéticos y mejorar las capacidades para "impedir y desbaratar los ataques en el Reino Unido". Un Centro de Control de seguridad y de operaciones globales y un grupo de operaciones de defensa cibernética del Ministerio de Defensa defienden respectivamente la red del Ministerio e integran las ciberactividades en todo el espectro de las operaciones defensivas. El Reino Unido anunció en 2013 su intención de incorporar la guerra cibernética como parte de futuras operaciones militares y desarrollar una *'cyber strike force'* para responder a un potencial uso militar de capacidades cibernéticas.

Reino de España

Si bien España pertenece a la Unión Europea, se ha dejado para lo último por constituir un caso especial debido a que, de lo que se ha podido indagar, aunque la Directiva de Defensa Nacional de 2012 dispuso la participación del Ministerio de Defensa en el impulso de una gestión integral de la ciberseguridad, en el marco de los principios que se establecen al efecto en la Estrategia de Ciberseguridad Nacional, este país, hasta donde se ha podido indagar, no dispone de una política o una estrategia de ciberdefensa como otros países de la Unión Europea.

Para resolver el problema, en enero de 2011, con el objeto de facilitar el desarrollo y empleo de las capacidades militares necesarias que permitiesen garantizar la eficacia en el uso del espacio cibernético en las operaciones militares, el Jefe del Estado Mayor de la Defensa (JEMAD) elaboró el documento "Visión del JEMAD de la Ciberdefensa Militar", en el cual se incluyó al espacio cibernético como uno de los dominios de enfrentamiento, siendo los otros tierra, mar, aire y espacio exterior. Asimismo, se dieron las orientaciones para definir, desarrollar y emplear las capacidades militares del país y, así, garantizar la eficacia en el uso del espacio cibernético en las operaciones militares[304].

Como resultado de ello, en julio de 2012 se aprobó el "Concepto de Ciberdefensa Militar", que definió principios, objetivos y retos de la ciberdefensa en el ámbito militar; en este documento, se define la terminología, se realiza una valoración de la capacidad, se presentan las funciones y responsabilidades en esta área, y se ordena la elaboración de un Plan de Acción de Ciberdefensa Militar. Un año después se anunció el "*Plan de Acción para la Obtención de la Capacidad de Ciberdefensa Militar*" (PACDM), con el cual comenzó la coordinación de los esfuerzos entre el ámbito conjunto y los específicos a partir del aprovechamiento de las estructuras existentes[305].

Para Francisco Zea Pasquín[306], este Plan de Acción:

> ...identifica las acciones necesarias para la obtención de una capacidad de Ciberdefensa Militar que cumpla con los objetivos especificados en el concepto de Ciberdefensa Militar, como son: garantizar el libre acceso al espacio cibernético con el fin de cumplir las misiones asignadas a las Fuerzas Armadas, obtener, analizar y explotar la información sobre ciberataques e incidentes en las redes y sistemas de su responsabilidad, y ejercer la respuesta oportuna, legítima y proporcionada ante amenazas, etc. El PACDM diseña una estrategia de obtención incremental que, empezando por una primera fase denominada Capacidad Inicial, relacionada directamente con la Capacidad de Defensa, obtiene la capacidad de resistencia ante los posibles ciberataques, así como a la recuperación de la funcionalidad de los sistemas ante los daños producidos por estos. Se pasará entonces a una segunda fase, denominada Capacidad

304 Mando Conjunto de Ciberdefensa, Reseña Histórica Disponible en: http://www.emad.mde.es/CIBERDEFENSA/historia/

305 España, Mando Conjunto de Ciberdefensa; Disponible en: http://www.emad.mde.es/CIBERDEFENSA/

306 Zea Pasquín, Francisco, "Ciberdefensa Militar" Revista Española de Defensa, marzo 2013, P. 48

Intermedia, en la que además de fortalecer la Capacidad de Defensa, se desarrollará la Capacidad de Explotación, orientada a la obtención de información sobre las capacidades de los posibles adversarios, unida a actividades de recopilación, análisis y explotación de esta.

Siguiendo con estos conceptos de Zea Pasquín, la tercera fase denominada Capacidad Final,

> ...se centra en la obtención de la Capacidad de Respuesta ante los ciberataques que se dirijan a los sistemas CIS de las Fuerzas Armadas. Una vez obtenidas las tres Capacidades (Defensa, Explotación y Respuesta), se puede afirmar que se dispone de una Capacidad de Ciberdefensa adecuada que complementará al resto de Capacidades Militares que poseen nuestras fuerzas armadas.

Con el objeto de potenciar la implementación de este Plan de Acción, el 19 de febrero de 2013, el Ministro de Defensa estableció la creación del Mando Conjunto de Ciberdefensa de las Fuerzas Armadas (MCCD),

> ...responsable de realizar el planeamiento y la ejecución de las acciones relativas a la ciberdefensa militar en las redes y sistemas de información y telecomunicaciones de las Fuerzas Armadas u otros que pudiera tener encomendados, así como contribuir a la respuesta adecuada en el espacio cibernético ante amenazas o agresiones que puedan afectar a la Defensa Nacional[307].

Nótese que se lo llama **Mando** porque al no tener unidades de ejecución que le dependen, sería impropio llamarlo **Comando**.

El ámbito de actuación del MCCD son las redes y los sistemas de información y telecomunicaciones de las fuerzas armadas, así como aquellas otras redes y sistemas que específicamente se le encomienden y que afecten a la Defensa Nacional.

La misión del MCCD es el planeamiento y la ejecución de las acciones relativas a la ciberdefensa militar en las redes y sistemas de información y telecomunicaciones de las fuerzas armadas u otros que pudiera tener encomendados, así como contribuir a la respuesta adecuada en el espacio cibernético ante amenazas o agresiones que puedan afectar a la Defensa Nacional.

Entre sus funciones se encuentran las de:

- Garantizar el libre acceso al espacio cibernético, con el fin de cumplir las misiones y cometidos asignados a las fuerzas armadas, mediante el desarrollo y empleo de los medios y procedimientos necesarios.

---

307 Exposición del coronel Roberto Villanueva Barrios. Jefe de Estado Mayor y 2º Comandante del MCCD, Seminario CDS sobre Ciberdenfesa - UNASUR, Buenos Aires mayo 2014; Disponible en: http://www.ciberdef.mindef.gob.ar/content/pdfs/bsas/Villanueva.pdf .

- Garantizar la disponibilidad, integridad y confidencialidad de la información, así como la integridad y disponibilidad de las redes y sistemas que la manejan y tenga encomendados.
- Garantizar el funcionamiento de los servicios críticos de los sistemas de información y telecomunicaciones de las Fuerzas Armadas en un ambiente degradado debido a incidentes, accidentes o ataques.
- Obtener, analizar y explotar la información sobre ciberataques e incidentes en las redes y sistemas de su responsabilidad.
- Ejercer la respuesta oportuna, legítima y proporcionada en el espacio cibernético ante amenazas o agresiones que puedan afectar a la Defensa Nacional.
- Dirigir y coordinar, en materia de ciberdefensa, la actividad de los centros de respuesta a incidentes de seguridad de la información de los Ejércitos y el de operaciones de seguridad de la información del Ministerio de Defensa.
- Ejercer la representación del Ministerio de Defensa en materia de ciberdefensa militar en el ámbito nacional e internacional.
- Cooperar, en materia de ciberdefensa, con los centros nacionales de respuesta a incidentes de seguridad de la información, de acuerdo con lo que determinen las estrategias y políticas nacionales de ciberseguridad en vigor, así como con otros centros militares de respuesta a incidentes de seguridad de la información en el ámbito internacional.
- Definir, dirigir y coordinar la concienciación, la formación y el adiestramiento especializado en materia de ciberdefensa.

Para Luis Feliú,[308] "es interesante resaltar que el error de confundir seguridad con defensa no se da en el "Concepto de Ciberdefensa del JEMAD" ya que en él define claramente a la ciberdefensa militar como "conjunto de recursos, actividades, tácticas técnicas y procedimientos para preservar la seguridad de los sistemas de mando y control propios y la información que manejan, así como permitir la explotación y respuesta sobre los sistemas adversarios, para garantizar el libre acceso al espacio cibernético de interés militar y permitir el desarrollo eficaz de las operaciones militares y el uso eficiente de los recursos."

Estados Unidos de Norteamérica

En el nivel operacional, los Estados Unidos de Norteamérica tienen la publicación Joint Publication JP 3-12 (R), *Cyberspace Operations,* que, en su última versión de febrero de 2013, incorpora al espacio cibernético y lo integra a las operaciones conjuntas, explica las operaciones en el espacio cibernético y su relación con las funciones conjuntas, establece las autoridades, roles y responsabilidades, y discute el planeamiento y la coordinación de las operaciones cibernéticas.

Clasifica a las operaciones en el espacio cibernético, sobre la base de sus intenciones como operaciones ofensivas del espacio cibernético (OCO), las operaciones defensivas

308 Feliú, Luis, Seguridad Nacional y Ciberdefensa: Aproximación Conceptual: Ciberseguridad y Ciberdefensa. Op. Cit.

del espacio cibernético (DCO), y las operaciones DODIN (Redes de Información del Departamento de Defensa). OCO son las que pretenden proyectar poder mediante el uso de la fuerza en y a través del espacio cibernético. DCO son aquellas que intentan defender el propio espacio cibernético o el de los aliados. Las operaciones DODIN son acciones tomadas para diseñar, construir, configurar, asegurar, operar, mantener y sostener sistemas de comunicaciones y las redes de Defensa de manera de poder crear y conservar la disponibilidad de datos, integridad y confidencialidad, así como la autenticación del usuario o entidad y el no-repudio[309].

Los comandantes integran las capacidades del espacio cibernético a todos los niveles y en todas las operaciones militares. Los planes deben referirse a cómo integrar eficazmente las capacidades del espacio cibernético, contrarrestar su uso por parte del adversario, asegurar las redes importantes para la misión, operar en un ambiente degradado, utilizar eficientemente los limitados activos del espacio cibernético y consolidar los requerimientos operacionales para las capacidades de este espacio.

Los denominados elementos de apoyo están organizados desde el US CYBERCOM y desplegados para integrarse a los Estados Mayores de los Comandantes. Este personal facilita el desarrollo de los requerimientos en el espacio cibernético y coordina e integra las operaciones cibernéticas en el proceso de planeamiento. Estos elementos de apoyo proporcionan una relación y una retroalimentación al USCYBERCOM para sincronizar los fuegos en el espacio cibernético con el esquema de maniobra del comandante, apreciar la situación y facilitar la adquisición de información oportuna de la amenaza. El US CYBERCOM mantiene el control operacional de estos Elementos de Apoyo y el CSE (*Ciber Support Element*) es un apoyo directo del Centro Ciberconjunto.

República Federativa de Brasil

En 2010, el Ministerio de Defensa de Brasil dispuso la creación, en el ámbito del Ejército, del Centro de Defensa Cibernética (CDCiber) con la misión de profundizar la prevención de las amenazas, establecer una doctrina nacional sobre el tema y perfeccionar los medios de defensa contra esas amenazas. Dicho Centro comenzó a desarrollar sus actividades de modo estratégico a partir de septiembre de 2012[310].

El 27 de diciembre de 2012, Brasil publicó su Política Cibernética de Defensa[311] la cual se elaboró, en el contexto de un acontecimiento social de envergadura como el Campeonato Mundial de Futbol de 2014 y en vistas al desarrollo de los Juegos Olímpicos previstos para 2016 en ese país. Esto es importante dado que el sostenimiento de las infraestructuras críticas frente a eventuales ataques demanda esfuerzos por parte

309 No repudio es el aseguramiento de que alguien no puede negar algo. Por lo general, el no repudio se refiere a la capacidad de garantizar que una de las partes de un contrato o en una comunicación no puede negar la autenticidad de su firma en el documento o el envío de un mensaje que ellos mismos originaron.

310 Brasil, Creación del CD Ciber, 2012 Disponible en: http://www.defesanet.com.br/cyberwar/noticia/5954/CDCiber---Centro-de-Defesa-Cibernetica-iniciaem-Junho

311 Brasil Política Cibernética de Defensa, Portaria Normativa No- 3.389/MD Disponible en: http://www.defesanet.com.br/cyberwar/noticia/9128/MD---Politica-Cibernetica-de-Defesa

de las autoridades. Nótese que, para entonces, la Estrategia Nacional de Seguridad Cibernética no había sido emitida.

Dicho documento tiene la finalidad de orientar, en el ámbito del Ministerio de Defensa, las actividades de Defensa Cibernética, en el nivel estratégico, y de Guerra Cibernética, en los niveles operacional y táctico, así como el control respecto de la consecución de los objetivos y atender las necesidades de la Defensa Nacional.

El documento "hace previsiones sobre acciones cibernéticas de carácter ofensivo y una definición respecto de que las acciones cibernéticas destinadas a asegurar la utilización del espacio cibernético e impedir o minimizar los efectos de ciberataques contra los intereses del país"[312] y entiende que la defensa cibernética consiste en adoptar acciones defensivas, exploratorias y ofensivas en el marco de una planificación militar, con el fin de proteger los sistemas de información, obtener datos para producir conocimiento e inteligencia y, eventualmente, causar daños a los sistemas de información enemigos.

Asimismo, propicia la "Producción de Conocimiento de Inteligencia" para crear "Estructuras de Inteligencia Cibernética" para detectar amenazas, reales y potenciales de carácter interno o externo.

Entre las medidas se destacan la creación, bajo la responsabilidad del Estado Mayor Conjunto, del Comando de Defensa Cibernética y de la Escuela Nacional de Defensa Cibernética. Asimismo, la Secretaría General del Ministerio de Defensa será responsable de decidir acerca de los recursos presupuestarios y de personal e infraestructura. Por su parte, el Ejército desarrollará la activación del Núcleo de Comando de Defensa Cibernética.

En 2014, fue publicada la "*Doutrina Militar de Defesa Cibernética* (MD31-M-07, 1ª Edição/2014)[313]", por medio de la Portaria normativa nº 3.010/MD, de 18 de noviembre de ese año.

En dicha publicación se señala que, desde el establecimiento del sector cibernético, resultantes de la aprobación de la Estrategia de Defensa Nacional, en 2008, fueron reconocidos dos campos separados: la Seguridad Cibernética a cargo de la oficina de la Presidencia de la República y la Defensa Cibernética, a cargo del Ministerio de Defensa, a través de las fuerzas armadas; y que en el contexto del Ministerio de Defensa, las acciones en el espacio cibernético deben tener las siguientes denominaciones, según el nivel de decisión:

- Nivel político - seguridad de información y las comunicaciones de ciberseguridad- coordinado por la Presidencia de la República y que abarca a la Administración Pública Federal directa e indirecta, así como las infraestructuras críticas de información nacionales;
- Nivel estratégico: Defensa Cibernética – a cargo del Ministerio de Defensa, fuerzas armadas y Estado Mayor Conjunto y comandos de las fuerzas armadas, que interactúan con la Presidencia de la República y la Administración Pública Federal; y

312 Uzal, Roberto, artículo Política de Defensa y Política Cibernética de Brasil, 5 enero 2013; Disponible en: http://espacioestrategico.blogspot.com.ar/2013/01/brasil-y-su-politica-cibernetica-de.html .

313 Brasil, Ministerio de Defesa, Doutrina Militar do Defesa Cibernética, MD 31 M 07; Disponible en: http://www.defesa.gov.br/arquivos/legislacao/emcfa/publicacoes/doutrina/md31_m_07_defesa_cibernetica_1_2014.pdf

› Niveles operacional y táctico - Guerra Cibernética - denominación restringida al ámbito interno de las fuerzas armadas.

En el capítulo 2 fija los fundamentos de la defensa cibernética entre los que se destacan los principios de empleo, las características, las posibilidades, las limitaciones, las formas de actuación y los tipos de acciones cibernéticas a los que clasifica como ataque cibernético, protección cibernética y exploración cibernética.

En el capítulo 3 se describe el sistema militar de defesa cibernética, los niveles de decisión, el concepto del Sistema Militar de Defensa Cibernética y los niveles de Alerta Cibernética.

En el capítulo 4 se dispone que en lo que respecta al nivel operacional, la Doctrina establece que la guerra cibernética puede ser planeada y ejecutada mediante el pedido de los efectos deseados por el Comando Operacional por grupos específicos designados para tal fin, empleando el canal técnico con los órganos responsables de la defensa cibernética de cada fuerza armada y del Ministerio de Defensa[314] y en principio, integrando células de Operaciones de Información[315], o a criterio del Comandante Operacional.

También, se describen las operaciones de información, el destacamento conjunto de defensa cibernética y los destacamentos de guerra cibernética y la forma en que debieran planearse la defensa y la guerra cibernética en las operaciones.

El destacamento conjunto de defensa cibernética, dependiente de CDCiber, en las operaciones actúa en un ambiente interagencial que requiere de una coordinación en el nivel estratégico, mientras que los destacamentos de guerra cibernética están directamente subordinados al Comandante Operacional a los efectos de[316]:

a. identificar y analizar las vulnerabilidades (conocidas) en redes de computadoras y aplicaciones empleadas en el sistema C^2 desplegado para la operación;
b. recomendar acciones para mitigar las vulnerabilidades identificadas;
c. estudiar las amenazas y entender su impacto en las redes de C^2 o cualquier otra estructura/recursos computadorizados de las fuerzas amigas;
d. verificar la conformidad de la Seguridad de la Información y Comunicaciones en el Sistema de C^2 desplegado para la operación;
e. planear y ejecutar acciones cibernéticas (protección, exploración y ataque), en el contexto de la operación conjunta, con apoyo de los órganos de Defensa Cibernética de las Fuerzas Armadas en cumplimiento de las orientaciones y directivas emanadas del Comando Operacional;
f. asesorar a los comandantes de los componentes, los pedidos de efectos deseado dirigidos al escalón competente para obtenerlos;
g. colaborar con la ejecución de las Operaciones de Información planeadas; y

314 Ibidem. P. 29/36.

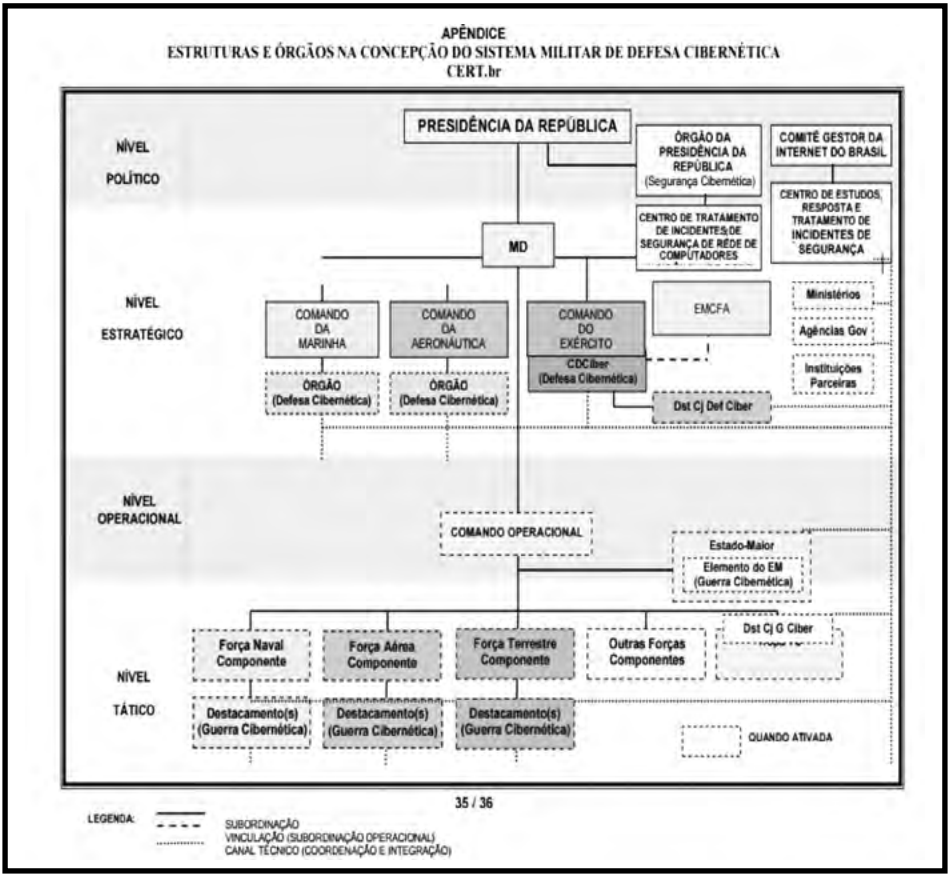
315 Ver figura 16.

316 Brasil, Ministerio de Defesa, Doutrina Militar do Defesa Cibernética, MD 31 M 07; Disponible en: http://www.defesa.gov.br/arquivos/legislacao/emcfa/publicacoes/doutrina/md31_m_07_defesa_cibernetica_1_2014.pdf P. 30/36

h. colaborar con el esfuerzo de obtención de datos para la producción de conocimiento de Inteligencia, por intermedio de la Fuente Cibernética[317], en el contexto de la operación conjunta, en cumplimiento de las orientaciones y directivas emanadas del Estado Mayor Conjunto.

En dicha Doctrina Conjunta también se muestra la organización del sistema militar de defensa cibernética que se muestra en la Figura 5.

FIGURA 5: ESTRUCTURA Y ORGANISMOS DEL SISTEMA DE DEFENSA CIBERNÉTICA DE BRASIL



Fuente: MD 31-M-0

317 Recurso por intermedio del cual se puede obtener dados en el Espacio Cibernético utilizándose acciones de búsqueda o colección, normalmente realizadas con la ayuda de herramientas computadorizadas. La Fuente Cibernética podrá ser integrada a otras fuentes (humanas, imágenes y señales) para la producción de conocimientos de Inteligencia.

República Argentina

Por Resolución 385/13 se dispuso la conformación de la Unidad de Coordinación Cibernética en el ámbito de la Jefatura del Gabinete de Asesores del Ministerio de Defensa, integrada por diferentes organismos del Ministerio de Defensa y las Fuerzas Armadas.

Por Resolución 343/2014, se creó el "Comando" Conjunto de Ciberdefensa con la misión de:

> ...ejercer la conducción de las operaciones de ciberdefensa en forma permanente a los efectos de garantizar las operaciones militares del instrumento militar de la defensa nacional en cumplimiento de su misión principal y de acuerdo a los lineamientos establecidos en el planeamiento estratégico militar.

También se le ordena que "deberá ser capaz de conjurar y repeler ciberataques contra las infraestructuras críticas de la información y los activos del Sistema de Defensa Nacional y de su Instrumento Militar dependiente".

Para Eissa[318] y otros autores, respecto de la actuación de las Fuerzas Armadas frente a potenciales ataques a través del ciberespacio y con la finalidad de delimitar los ámbitos de actuaciones de las fuerzas armadas, debido a que es *casi* (sic) imposible identificar quién es el agresor, y considerando como punto de partida a la legislación y doctrina vigente en la materia,

> ...creemos que debe adoptarse un enfoque basado en efectos. Es decir, la intervención del Sistema de Defensa en el ciberespacio debe estar definida no por quien produce el ataque, sino en base a qué infraestructura o sistema está siendo afectado. En función de lo expuesto, consideramos que el Sistema de Defensa Nacional debe:
>
> - adherir al Programa Nacional de Infraestructura Crítica de Información y Ciberseguridad a los efectos de poner en funcionamiento las normas y medidas que permitan incrementar la seguridad de las redes del sistema;
> - garantizar la seguridad de las redes informáticas del Sistema de Defensa nacional;
> - garantizar la defensa contra aquellos ciberataques que pretendan obstaculizar las operaciones militares del Instrumento Militar en cumplimiento de su misión principal; y
> - tener capacidades para realizar operaciones cibernéticas de defensa indirecta en el ciberespacio.
> - En este sentido, sólo en tiempos de guerra, el Instrumento Militar debe estar preparado también para repeler y conjurar un ciberataque perpetrando los objetivos estratégicos definidos por el Ciclo de Planeamiento de la Defensa Nacional (Decreto 1729/2007).

---

318 Eissa, Sergio G., Gastaldi, Sol, Poczynok, Iván y Zacarías Di Tullio, María Elina, El ciberespacio y sus implicancias en la defensa nacional. Aproximaciones al caso argentino. Op. Cit.

Este aislamiento del componente militar del poder nacional que se propugna en el contenido de este documento es un ejercicio ideológico inútil para el fin que se busca que, justamente, es la seguridad de la nación ante agresiones cibernéticas. La conclusión es que, si el componente militar debe hacer frente a las agresiones cibernéticas militares externas de otros estados, pero como también se sostiene que es "casi imposible identificar al agresor", en los hechos se vacía de contenido a la cibernética militar.

Conclusiones del capítulo

Como ha podido apreciarse, en concordancia con las respectivas Directivas de Defensa Nacional, los países analizados elaboran sus correspondientes doctrinas militares de Defensa Cibernética y al mismo tiempo crean *Comandos* de Ciberdefensa, o bien, si aún no tienen elementos de ejecución como organizaciones de detección de redes o de respuesta inmediata, crean *Mandos* o *Centros*, con la finalidad de coordinar estrategias, políticas y procedimientos dentro de las fuerzas armadas.

A su vez, estos comandos/mandos/centros de Ciberdefensa son quienes llevan a cabo las operaciones cibernéticas, requeridas en forma de efectos a lograr por los Comandantes de Teatro, quienes cuentan, en su Estado Mayor, con elementos de apoyo provistos por aquellos.

En nuestro país se ha creado el Comando Conjunto de Ciberdefensa, pero aún no se elaboró ni la Estrategia de Seguridad Nacional, ni la de Ciberseguridad ni la de Defensa Nacional. Por su parte, dado que la legislación vigente no acepta las denominadas "nuevas amenazas" y que, por ende, estas no pueden trasladarse directamente al Sistema de Defensa argentino, la elaboración de una Doctrina Militar de Ciberdefensa seguramente será algo complicado de lograr.

Al ponerse en duda la identificación de una dimensión específicamente militar del ciberespacio, como lo hace la DPDN, en tanto no es posible –al menos en la actualidad– establecer cuáles son los alcances reales de las operaciones cibernéticas, parecería que los llamamientos a militarizar el ciberespacio son más una reacción ante la incertidumbre que el resultado de análisis estratégicos pormenorizados, sustentados empíricamente.

Esta es una afirmación ideológica falaz. **Militarizar** el ciberespacio está en la mente de quienes redactaron este informe. En el ciberespacio conviven todas las actividades del ser humano, y también puede ser usado con fines militares, pero no exclusivamente. El uso de la cibernética en los reactores nucleares de Irán, en Estonia, en la guerra Rusia-Georgia y en la guerra Rusia – Ucrania son una muestra.

En general, el plan de acción ha sido la creación de Comandos (si tuvieran elementos de ejecución que les dependiese) o Centros, o Mandos Conjuntos de Defensa Cibernética, dentro de una Política de Defensa Nacional y una Estrategia de Defensa Cibernética, que integra las acciones privadas y públicas, con un ámbito específico para los sectores militares. En el caso de la Argentina, se ha comenzado por abajo.

Desarrollar una doctrina abarcadora de guerra cibernética es una tarea compleja que requiere muchos cuidados. A pesar de que, tanto civiles como militares han progresado considerablemente hacia asegurar sus infraestructuras nacionales y prepararse para la guerra en el espacio cibernético, desafortunadamente, estos esfuerzos están siendo desa-

rrollados e implementados de manera gradual. Los intereses civiles y militares son muchas veces separados e inconexos, independientemente de la buena disposición que ambos lados puedan tener para crear una sinergia entre ambos. Las ideologías remanentes de la Guerra Fría juegan un rol importante en esta separación y falta de integración.

Se carece de un verdadero enfoque sistémico para manejar los conflictos originados en el espacio cibernético que cruzan muchos intereses y límites jurisdiccionales. Lo que se necesita es una política nacional sobre cómo manejar los ataques basados en las Tecnologías de la Información que puedan llegar a perturbar el funcionamiento normal del país. Dicha política debería incorporar un conjunto de principios de autodefensa que incluya la infraestructura civil y los objetivos militares y una Política de Seguridad Nacional. Para ello, debe establecerse una Doctrina de Ciberdefensa que se utilizaría para determinar la respuesta apropiada de la nación cuando sea atacada vía el espacio cibernético. Tal doctrina serviría como guía para las fuerzas armadas en tiempo de conflicto; como una filosofía de gobierno unificada para las operaciones militares, y se implementaría para proteger la infraestructura civil y la gobernanza de las relaciones internacionales cibernéticas; y como un elemento disuasivo para futuros adversarios.

Sin embargo, actualmente no existen teóricos militares especializados en guerra cibernética, como en su momento fueron Alfred Thayer Mahan, Giulio Douhet y B.H. Liddell Hart que razonaron respectivamente sobre los dominios marítimo, aéreo y terrestre, generando marcos, modelos y principios para la guerra. En la actualidad, estas teorías ayudan a los estrategas y planificadores a pensar, planificar y generar las fuerzas de combate conjuntas, pero, no existe ninguna teoría militar estándar para las operaciones en el espacio cibernético y la teoría militar es un componente primario del arte operacional.

La doctrina militar actual analiza las experiencias y teorías de la guerra cinética entre las naciones- estados en espacios de batalla que existen casi exclusivamente en una zona físicamente reconocible y comprensible (aire, tierra, mar y espacio) pero, contrariamente a ello, la guerra cibernética ocurre en un ámbito ubicado simultáneamente en capas lógicas y físicas que cruzan actividades en el espectro electromagnético (y a través de este) que atraviesa ininterrumpidamente otros ámbitos al igual que fronteras geográficas y políticamente reconocidas.

A pesar de este panorama incierto, se puede afirmar que la guerra cibernética es como dijeron los pensadores militares desde hace mucho tiempo: no hay guerra parecida a la anterior, sino que se pueden extraer algunas conclusiones.

La guerra cibernética difiere fundamentalmente del conflicto armado tradicional pues, a diferencia de la conducción de la guerra en el pasado, los oponentes pueden librar una guerra cibernética rápida, económica, anónima y devastadora, desde lugares apartados del globo. Un ataque cibernético puede originarse desde cualquier parte y por cualquiera, incluso por "piratas informáticos" auspiciados por un estado, actores no estatales o "trabajadores por cuenta propia" motivados políticamente.

La participación en la guerra cibernética no está limitada a los agentes del Estado. A diferencia del ataque militar convencional, llevar a cabo un ataque en el espacio cibernético no requiere el patrocinio del gobierno. El agresor no necesita sistemas de armamento tradicionales costosos.

Con la conectividad global del espacio cibernético no es necesario que un enemigo se encuentre próximo físicamente para planear y ejecutar una amenaza. Si los hackers pueden acceder a un sistema y obtener el control de funciones del teclado, pueden ocultar sus logros, eludir las defensas y dejar abiertas las puertas para volver a entrar en el futuro.

De manera similar a lo que sucede en otros dominios, como el aire y el mar, en el espacio cibernético no es posible defender todo; se debe defender lo que es relevante para las operaciones. "El que pretenda defenderlo todo termina por no defender nada." [319]

Se puede afirmar entonces que es necesario elaborar una doctrina de Ciberdefensa, en la cual se señalen al menos, los principios, las características, las posibilidades y limitaciones y los tipos de operaciones cibernéticas y que, para cada nivel de la guerra, se especifiquen las misiones y tareas a cumplir y se describa la estructura y organización que deberá adoptarse, en la cual se le deberá otorgar participación a los Estados Mayores Generales.

Hasta tanto no se elabore la Política o Estrategia Nacional de Seguridad Cibernética, el Jefe del Estado Mayor Conjunto podría emitir una Directiva de Defensa Cibernética, aprobada por el Ministerio de Defensa, haciendo mención de que debiera ser revisada anualmente para ajustarse a la que llegue a ser emitida.

De dicha Directiva se desprenderían, no solo el Plan de Desarrollo de Capacidades operacionales en la dimensión ciberespacial, descomponiendo cada una de ellas en los elementos que las conforman, – material – infraestructura – recursos humanos – información – logística – adiestramiento – doctrina – organización, según lo dispuesto en la Directiva de Política de Defensa Nacional (decreto 2645/2014), sino también otros documentos como el Plan de Concientización en Ciberdefensa para el personal integrante de las Fuerzas Armadas, el Plan de Reclutamiento; el Plan de Formación, el Plan de Carrera del personal y la Doctrina Conjunta de Ciberdefensa.

Lo que se ha hecho hasta el momento en los dominios tradicionales no tendrá mucha aplicación en este nuevo dominio cibernético. Para poner un ejemplo, un Plan de Carrera de un oficial del cuerpo de comando le impone pasar obligatoriamente por ciertos destinos administrativos que, de no cumplirse, no le permite acceder al grado superior. Entonces, no tendría sentido capacitar a un oficial en operaciones cibernéticas para obligarlo luego a pasar por algún destino burocrático al solo efecto de que cumpla el plan de carrera. Si esta situación se modificara, se podría crear, por ejemplo, el Cuerpo Cibernético, o el Cuerpo Informático, o cualquier otro nombre que se le quiera poner, con un Plan de carrera específico.

319 Apotegma atribuido a Federico el Grande. Citado por Ferdinand Foch en su Libro "Los principios de la guerra"

CAPÍTULO 4

LAS OPERACIONES MILITARES EN EL ESPACIO CIBERNÉTICO

Introducción

Cuando un estado es atacado por tierra, mar o aire por fuerzas convencionales, está clara la manera de responder empleando medios, estrategias y tácticas tradicionales. Sin embargo, surgieron nuevas preguntas: ¿qué sucede cuando un ataque es perpetrado con una mezcla de fuerzas especiales, operaciones de información y redes de robots informáticos o *botnets*, que se ejecutan de manera autónoma y automática y lanzan ataques usando computadoras situadas en un país desconocido, o incluso desde el propio territorio? ¿cuál es la mejor respuesta?; ¿cómo es posible responder a estos ataques dado que existe el riesgo que el estado afectado pueda ejercer represalias sobre alguien totalmente ajeno a los hechos?

Todo esto afecta a los militares, especialmente cuando deben cumplir con su función específica de defender la soberanía territorial y el bienestar de los habitantes del Estado al que pertenecen, pero también a los propios Estados, pues ellos, a pesar de que el espacio cibernético carece de fronteras, son plenamente responsables del funcionamiento de sus medios de telecomunicaciones e informática dentro de sus fronteras.

Ante ello, y como se ha visto hasta este punto de la investigación, los países se organizan a partir de una Estrategia de Seguridad y Defensa Nacional para arribar, previo a la redacción de una doctrina de ciberdefensa, a la conformación de un Comando/Mando/Centro Conjunto de Ciberdefensa, el cual, a la vez que interactúa con cada una de las fuerzas armadas, a través de elementos de apoyo que organiza, participa del planeamiento y ejecución de las operaciones que son responsabilidad del Comandante de Teatro y, por medio de las capacidades que dispone, trata de alcanzar los efectos que le fueran requeridos por éste.

También, se ha podido apreciar en esta obra, en qué consiste un ataque cibernético y que las operaciones cibernéticas se clasifican en ofensivas, defensivas (pasivas y ac-

tivas) y de exploración. Resta ahora ver cómo emplearlas dentro del nivel operacional. Antes de entrar de lleno en ello, se exponen algunas consideraciones.

La primera de ellas es que mientras en el siglo XX la superioridad tecnológica descansaba principalmente sobre el industrialismo, a comienzos del siglo XXI ese modelo cambió hacia la informática. Quedó así atrás la definición que el General francés André Beaufre[320] daba a la **estrategia genética o estrategia logística**, consistente en el desarrollo de armamento superior al que tuvieran los eventuales oponentes[321].

Una clave para identificar la transición entre el industrialismo y la informática puede encontrarse en las declaraciones del ex Secretario de Defensa de los Estados Unidos William Perry[322] (período 1994-1997) en su entrevista con académicos chinos luego de la Guerra del Golfo I, cuando expresó: "Lo que han sido importantes logros de revolución militar tecnológica han sido naturalmente las técnicas furtivas y las tecnologías de información".

La segunda consideración es que la cibernética proporcionó armas a los más débiles en fuerzas convencionales, por lo tanto, puede inferirse que favoreció la guerra asimétrica. Se puede usar en forma anónima, y la disuasión y la represalia son dificultosas; además, sus efectos inmediatos son no letales, de manera tal que el riesgo de escalada se reduce.

En tercer lugar, se debe ser cuidadoso al comparar con otros países. Naturalmente, existe una tendencia a comparar con Estados Unidos y se olvida una disparidad de medios y organizaciones. Para poner un ejemplo, los conocidos como Comandos Unificados (antes CINC) son extensiones del nivel operacional, y no necesariamente cada Comando Unificado representa un Teatro de Operaciones, sino que dentro de un Comando Unificado pueden existir uno o más Teatros de Operaciones de la forma en que se los concibe en la Argentina.

Hechas estas salvedades, en esta investigación se define como poder cibernético militar: "... la aplicación del espacio cibernético a los conceptos operacionales para cumplir con los objetivos militares y las misiones, incluyendo todo el espectro del conflicto: asistencia humanitaria, desastres naturales, estabilización, crisis y guerra"[323].

La estructura piramidal del poder cibernético militar

La estructura del poder cibernético militar se representa por un triángulo cuya base descansa en las redes abiertas y cerradas y sus atributos, seguridad y resiliencia, con conectividad confiable, con alto ancho de banda, ágil y protegidas.

---

320 Beaufre André, Introducción a la estrategia, Traducción al español de la Editorial Struhart y Cia, Año 1962, Capítulo Primero, Visión general de la estrategia, Subdivisiones de la estrategia, P. 25.

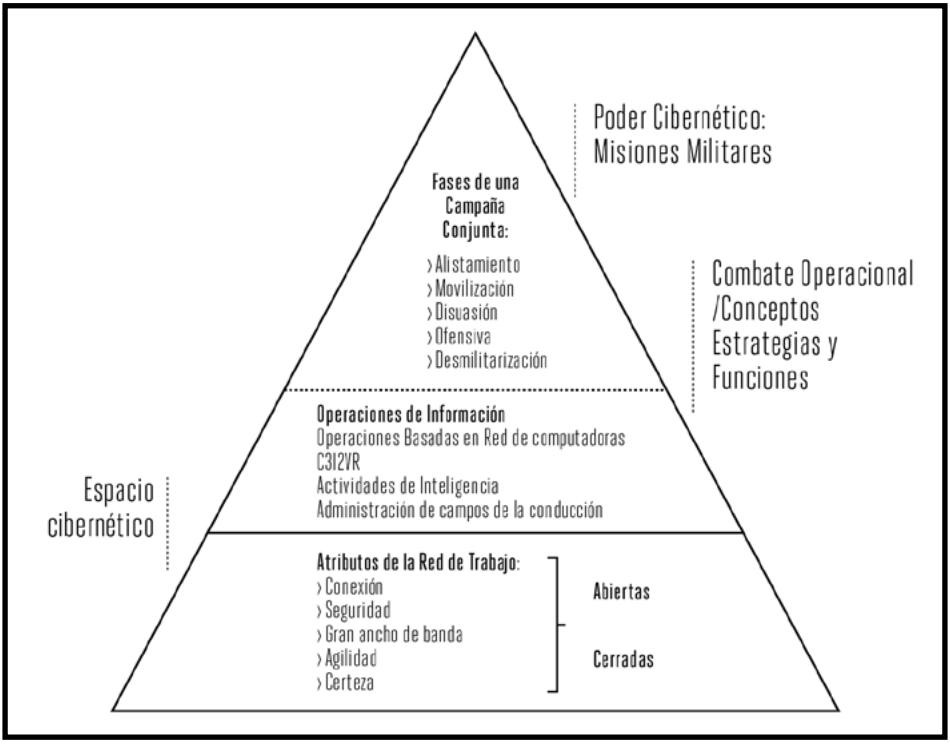
321 En este punto vale aclarar que, en la Argentina, por razones que se desconocen, se asoció estrategia genética al significado de adquisición de nuevos materiales, transformándose por falsa asociación o mala interpretación idiomática en la frase logística genética. Esto es una interpretación capciosa, caprichosa y falaz de la frase original acuñada por el General Beaufre.

322 Citado por QuiaoLiang y Wang Xiangsui, Unrestricted Warfare – China´s plan to destroy America – Pan American Publishing Company, Panama City, Año 2002, Part Two, A Discussion of a new Method of Operation, P. 93.

323 Zimet, Elihu and Barry, Charles L. "Military Service Overview" en Kramer, Franklin D., Starr, Stuart H. and Wentz, Larry K., Editors, Cyber power and National Security, National Defense University Press and Potomac Books, P. 290

En el nivel intermedio, se implementan los conceptos operacionales, estrategias y funciones que incluyen las operaciones basadas en redes de computadoras (NCO) y las operaciones de información, pero también funciones administrativas como, por ejemplo: la logística, el planeamiento, el entrenamiento, las adquisiciones y el manejo y administración del personal. El ápex del triángulo incluye las misiones militares y su relación con el poder cibernético militar, es decir, el uso del poder cibernético en todas las fases de una campaña.

FIGURA 6: ESTRUCTURA DEL PODER CIBERNÉTICO MILITAR[324]



Los sistemas cibernéticos cerrados o abiertos

Los sistemas cibernéticos militares pueden ser de dos tipos bien diferentes: abiertos o cerrados.

Los sistemas cibernéticos abiertos son las redes accesibles para cualquier usuario que desee ingresar, con clave de identificación. La seguridad de una red abierta está en ese acceso con clave, encriptado y en herramientas de protección comerciales. Por lo ge-

324 Ibidem, P. 293

neral, son vulnerables a infecciones de malware producto del uso de Internet, o a fallas de seguridad en los sistemas operativos. Las principales medidas de rendimiento en los sistemas cibernéticos abiertos son la conectividad, la disponibilidad y el ancho de banda. Debido a la vulnerabilidad de los sistemas abiertos que dependen de los sistemas comerciales, es que las fuerzas militares se esfuerzan por desarrollar sus propios sistemas para reducirlos.

En los sistemas abiertos, tiene importancia la colaboración en compartir la información y las medidas de rendimiento y conectividad. La vulnerabilidad más importante de los sistemas cibernéticos abiertos es su dependencia, tanto en productos como en servicios, de las capacidades civiles en el espacio cibernético.

Los sistemas cibernéticos militares cerrados existen, aunque no todavía en la Argentina. Una red cibernética cerrada tiene acceso solamente para los nodos autorizados y están aisladas de las redes abiertas. Las principales medidas de rendimiento de las redes cerradas son seguridad, disponibilidad y certeza en la información que se trasmite. Los sistemas cibernéticos cerrados son vulnerables a infecciones o programas maliciosos introducidos vía un USB drive.

Las actividades en el ciberespacio pueden permitir libertad de acción para las actividades en los otros dominios y estas, a su vez, pueden crear efectos en y a través del ciberespacio. A pesar de que las redes en el ciberespacio son interdependientes, partes de estas redes son aisladas. El aislamiento en el ciberespacio existe a través de protocolos, firewalls, encriptación y separación física de otras redes. Por ejemplo, existen redes clasificadas, como la denominada *US Armed Forces Secure Internet Protocol Router network* (SIPRnet)[325] que no están conectadas a Internet en todo momento, pero que pueden hacerlo y conectarse a través de portales seguros. Además, la construcción de algunas redes cableadas, las aísla de la mayoría de las formas de interferencia de radiofrecuencia (RF). Estos factores permiten a estas redes quedar aisladas en el ciberespacio, pero también conectarse a las redes globales[326].

Si bien pueden usar conectividad comercial, en el caso de sistemas cerrados los militares son los que controlan el acceso, los nodos y el tráfico, por ejemplo, para Estados Unidos, el *Secret Internet Protocol Router Network and Secure Telephone Units*[327].

Ambos sistemas militares cibernéticos participan en las operaciones militares mejorando sustancialmente las prestaciones derivadas del correcto uso de la información, aunque, como fuera dicho, deben ser seguras y resilientes.

Establecer una postura de defensa cibernética resiliente no es algo fácil de lograr, ya que requiere de prácticas de seguridad personal, de una arquitectura e ingeniería adecuada y de capacidades y soluciones para resolver rápidamente las deficiencias en la in-

---

325 La Argentina no posee satélites militares y las bandas anchas son alquiladas a empresas civiles. Se carece de información –por ser altamente clasificada– acerca de cuántas infraestructuras críticas poseen sistemas de control cerrados. Se dice que en la Argentina hay dos canales del satélite ARSAT de uso exclusivo militar, pero esta información probablemente sea clasificada, por lo que es contradictoria según las fuentes.

326 Introduction to Cyberspace Operations; Disponible en: https://fas.org/irp/doddir/usaf/3-12-annex.pdf

327 Cyberpower and National Security, Edited by Kramer, Starr and Wentz, Center for Technology and National Security Policy, National Defense University Press and Potomac Books, Washington DC, 2009, Página 287

fraestructura crítica y en los sistemas de información. Eso incluye, en primera instancia, poseer un sistema criptográfico sumamente robusto para proteger la integridad y confidencialidad de los datos e incrementar las exigencias de las políticas de adquisiciones de manera de garantizar que la seguridad informática sea un condicionante esencial al momento de decidir entre uno y otro equipo.

También requiere poseer adecuadas capacidades de defensa cibernética y mejorar el conocimiento de la situación en el espacio cibernético. Un ataque cibernético puede ocasionar que armas, misiles y bombas fallen o sean dirigidos contra las propias tropas, que las cadenas logísticas se interrumpan ocasionando escasez de alimentos, agua y municiones, que las cargas de los contenedores logísticos se confundan, que los planes de transporte se alteren, y que los abastecimientos y el mantenimiento no se hagan en tiempo y forma.

Las operaciones de red de computadoras y las operaciones de información

Una pregunta muy común que suele escucharse es ¿cuál es la diferencia entre operaciones de información y las operaciones de red de computadoras?

El espacio cibernético, al mismo tiempo que le otorga poder a quienes conecta mediante el acceso a caudales de información, también les introduce vulnerabilidades como, por ejemplo, la presentación en tiempo real de información sobre los conflictos difundida por ciudadanos y observadores sobre el terreno. Ello limita la acción de los ejércitos y sus servicios de comunicación, así como la eficacia en el mantenimiento del secreto. La multiplicación de mensajes a través de las redes sociales hace más compleja y difícilmente controlable la información y la desinformación. La aparición de grupos anónimos organizados en la red puede desestabilizar y generar situaciones caóticas en perjuicio de los intereses estratégicos.

A pesar de que ambas, información y desinformación, ocurren en el ambiente de la información, las operaciones de información y las operaciones cibernéticas, si bien están relacionadas representan dos conceptos distintos. Específicamente, las operaciones cibernéticas son actividades en el espacio cibernético y a través de este que permiten alcanzar la libertad de maniobra y lograr objetivos militares. Habida cuenta de su evolución en el tiempo, pueden crear efectos en el ambiente de la información.

Por su parte, las operaciones de información abarcan capacidades específicas que afectan la toma de decisiones de ciertas audiencias, al tiempo que protegen los procesos propios de toma de decisiones, ya que lo que persiguen es hacer equivocar al enemigo en las decisiones que tome.

Las operaciones cibernéticas están relacionadas con el uso de las capacidades del ciberespacio para crear efectos que apoyan las operaciones a través de los dominios físicos y el ciberespacio. Las operaciones de información se refieren más específicamente al empleo integrado de las capacidades relacionadas con la información durante las operaciones militares, en concierto con otras líneas de operación (LOOs) para influir, alterar, corromper o usurpar la toma de decisiones de adversarios y potenciales adversarios al mismo tiempo que se protegen las propias. Así, el ciberespacio es un medio a través del cual algunas capacidades relacionadas con la información, como las operaciones de

información militar en apoyo de las operaciones (MISO) o el engaño militar (MILDEC), pueden ser empleados. Las operaciones de información también utilizan las capacidades de los dominios físicos para lograr sus objetivos[328].

Cuando las operaciones cibernéticas se emplean en apoyo de las operaciones de información tratan de negar o manipular la toma de decisiones del adversario o potencial adversario, atacando un medio de información (como por ejemplo un punto de acceso inalámbrico en la dimensión física), el mensaje mismo (un mensaje cifrado en la dimensión de la información), o una ciber-persona (una identidad en línea que facilita la comunicación, toma de decisiones y la influencia de las audiencias en la dimensión cognitiva).

El empleo de las capacidades cibernéticas en las operaciones de información se trata en detalle en el Capítulo 6.

Las operaciones cibernéticas en red de computadoras

Como fue explicado en el capítulo 1, las operaciones de red de computadoras están dirigidas a modificar los datos y algoritmos de una red o sistema, para que se obtengan resultados contrarios a los que se esperaban. Estas operaciones son clasificadas por la mayoría de los países en ofensivas, defensivas (pasivas y activas) y de explotación o exploración de redes de computadoras. Los Estados Unidos las denominan *Computer Network Operations* y países como Gran Bretaña incluyen dentro de ellas a las operaciones de Ciberinteligencia, Vigilancia y Reconocimiento y las de ciberpreparación operacional del medio ambiente.

Las ofensivas existen y, aunque en un principio nadie estaba dispuesto a aceptar su uso, Australia ha reconocido públicamente que lleva a cabo operaciones cibernéticas ofensivas sobre ISIS. También, los medios de prensa dan cuenta de la colaboración de grupos de hackers *Ghost Security Group* con autoridadades estadounidenses para combatir al terrorismo islámico[329].

La mayoría de las operaciones ofensivas tienen efectos inmediatos solamente sobre los datos o el buen funcionamiento de la computadora de un adversario, reduciendo su conexión a la red, saturando la pantalla con corriente estática o mezclando los resultados de los cálculos básicos. Cualquiera de ellos podría tener un efecto militar si lograran que el adversario llegase a modificar equivocadamente el momento de un ataque, perdiese el control de una computadora o calculase mal las posiciones de un blanco.

Un ejemplo de operaciones ofensivas de redes de computadoras es el denominado "*Quantum Insert Attack*"[330,331] que surgió en las noticias como una de las diez más grandes

---

328 Joint Publication 3-12 (R), Cyberspace Operations, 5 February 2013, P. I-5 Disponible en: http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf

329 Esquivada Gabriela, Hackers vs. ISIS: cómo es la guerra tecnológica contra el terrorismo, Diario Infobae, martes 31 de enero de 2017; Disponible en: http://www.infobae.com/america/eeuu/2016/07/10/hackers-contra-isis-como-es-la-guerra-tecnologica-contra-el-terrorismo/

330 INFOSEC Institut. Analyzing Quantum Insert Attacks; Posted in Exploit Development, General Security, Hacking on May 7, 2015 Disponible en: http://resources.infosecinstitute.com/analyzing-quantum-insert-attacks/.

331 Un ataque Quantum es un ejemplo clásico de los que se conocen como ataques "man in the middle", (MitM o intermediario, en español) en el cual, como su nombre lo indica, el atacante se mantiene entre dos partes, haciéndoles creer que están hablando directamente el uno al otro mediante una conexión privada, cuando en realidad la conversación está siendo controlada por el atacante.

fugas de información debido a "*WikiLeaks*". Una vez que los servidores de *Quantum* alcanzan el objetivo, el atacante puede robar datos confidenciales, como credenciales, datos bancarios, números de tarjeta de crédito o incluso propagar un malware que puede funcionar en tándem con un servidor botnet de Comando y Control.

Hay que diferenciar la guerra cibernética de la guerra electrónica. Un ataque a drones puede ser hecho de las dos formas.

Por ejemplo, con técnicas de guerra cibernética,[332] pueden ser llevados a cabo mediante técnicas[333] tales como:

- Ataques tipo *spoofing* al sistema GPS – Los atacantes envían al sistema de control del drone falsas coordenadas geográficas para engañar al sistema de a bordo, secuestrar al vehículo y conducirlo a un lugar diferente al que se lo desea enviar.
- Ataques cibernéticos basados en malware – cualquier componente de software que se ejecuta en un drone podría ser golpeado por códigos maliciosos capaces de explotar una vulnerabilidad en sus sistemas.

La amenaza es concreta y probablemente ya sucedió en las redes militares de Estados Unidos. En octubre de 2011, la revista Wired informó que un virus infectó el sistema de control remoto de un drone; en particular el malware capturaba los trazos de un teclado en las cabinas de aviones en la Base de la Fuerza Aérea de Creech en Nevada, haciendo difícil para los pilotos el control remoto de drones como el Predator y el Reaper. El malware utilizado no parecía demasiado sofisticado pero los expertos en seguridad demoraron un par de semanas para inmunizar completamente el sistema[334].

Con técnicas de guerra electrónica, puede hacerse lo siguiente:

- Interferencias a la señal del GPS – los atacantes, usando técnicas de *jamming*, interrumpen el sistema de recepción de datos GPS de a bordo transmitidos al vehículo no tripulado (UAV). En este escenario, el drone puede perder potencialmente la capacidad de controlar su ruta y calcular su ubicación, altitud y la dirección en la que está viajando. Con esta técnica es posible forzarlo a aterrizar de manera segura, sin que se destruya.
- Ataques de pulso electromagnético (EMP) – los atacantes impactan el vehículo con una ráfaga corta de energía electromagnética que puede originarse bajo la forma de una radiación eléctrica, de un campo magnético o mediante una corriente

332 INFOSEC Institut Hack-Proof Drones Possible with HACMS (High Assurance Cyber Military Systems) Technology; Posted in General Security on June 3, 2014; Disponible en: http://resources.infosecinstitute.com/hack-proof-drones-possible-hacms-technology/.

333 También existen métodos mediante los cuales, por medio de un drone que vuela buscando la señal inalámbrica de cualesquiera otros drones, mediante un ataque de denegación de servicios, desconecta de su guiador a aquellos que localiza y se conecta a ellos tomando el control ("Técnicas hacking aplicadas a drones" Disponible en: https://noticiasdeseguridadinformatica.wordpress.com/2015/09/24/tecnicas-hacking-aplicadas-a-drones/.

334 INFOSEC Institut Hack-Proof Drones Possible with HACMS Op. Cit.

> eléctrica, según la fuente utilizada para el ataque. Los efectos que se buscan con este tipo de ataques de EMP es interferir o dañar los equipos electrónicos de los aviones no tripulados.

Ello es posible, pues prácticamente todos los componentes de estos vehículos pueden verse afectados por una *"vulnerabilidad generalizada"*[335] que los expone a los riesgos concretos de un secuestro.

Cabe mencionar que como cita Herr[336],

> una de las principales ventajas de los militares de Estados Unidos ha sido su red mundial de comando y control, con el sistema de posicionamiento global (GPS) que es una parte clave de la arquitectura que permite a las fuerzas operar con increíble precisión. Pero esa dependencia marca un aspecto clave del blanco. En 2010, una falla del software afectó 10.000 receptores GPS militares dejándolos fuera de línea durante más de dos semanas.

Las operaciones ofensivas en el espacio cibernético pueden afectar potencialmente cualquier cosa que implique tecnología informática o de comunicaciones, un hecho que los hace instrumentos extraordinariamente flexibles para llevar a cabo los deseos de los responsables de la política nacional y por el cual, muchas naciones, incluidas las más grandes y poderosas del mundo, están interesadas en explotar el valor potencial de este tipo de operaciones.

Para Mercy A. Kuo[337], las operaciones ofensivas en el espacio cibernético se ejecutan para comprometer la confidencialidad, la integridad o la disponibilidad de información. El hecho de que terceros no autorizados accedan a la información que no deberían tener, como por ejemplo robar registros médicos electrónicos, implica un compromiso para la confidencialidad de la información. El hecho de modificar un registro médico del tipo de sangre de un paciente que se presenta como tipo A, cuando su actual tipo de sangre es tipo O, compromete la integridad de la información. Así también imposibilitar el acceso a un expediente médico afecta la disponibilidad de la información.

Una nación puede elegir llevar a cabo operaciones ofensivas por muchas razones. Por ejemplo, tal vez desee recabar inteligencia sobre potenciales adversarios, en cuyo caso podrían utilizarse las operaciones ofensivas para espiar en el espacio cibernético. Tal vez desee interrumpir las operaciones de sistemas de armas del adversario, en cuyo caso

---

335 El concepto de "vulnerabilidad generalizada" (pervasive vulnerability) es ampliamente discutido y es objeto de estudios por varias entidades, incluyendo la Defense Advanced Research Projects Agency, (DARPA) y no se relaciona sólo UAVs, debido a que dichas debilidades afectan también los sistemas SCADA (Supervisory Control And Data Acquisition), dispositivos médicos, periféricos y dispositivos de comunicación.

336 Herr, Trey and Herrick, Drew, Military Cyber Operations: A Primer, The American Foreign Policy Council Defense Technology Program Brief, January 2016; Disponible en: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2725275

337 Kuo, Mercy A. Cybersecurity in US Asia Policy, October 08, 2016; Disponible en: http://thediplomat.com/2016/10/cybersecurity-in-us-asia-policy/

podría comprometer la integridad de las bases de datos utilizadas para controlar dónde y cuándo el adversario puede utilizar sus armas. O, tal vez desee causarle al adversario algunas interferencias temporales a modo de advertencia, en cuyo caso podría comprometer la disponibilidad de los sitios *home banking* del adversario.

Por ejemplo, informes periodísticos citados por Kuo, indicarían que:

> NanHaiShu sería un arma cibernética utilizada por hackers chinos (posiblemente financiados, apoyados o incentivados por el gobierno) para comprometer la confidencialidad de los archivos de organizaciones que se oponen a los reclamos en Mar del Sur de la China, de manera tal de poder conocer sus futuros movimientos[338].

Por su parte, las operaciones defensivas (activas y pasivas) se emplean para preservar la capacidad de utilizar el espacio cibernético propio y proteger datos, redes y otros sistemas determinados. Las medidas defensivas incluyen acciones para rápidamente restablecer, volver a asegurar, re- direccionar, reconstituir, o aislar aquellas redes que hayan sido degradadas o comprometidas, de manera de poder asegurar el acceso al espacio cibernético de las fuerzas en campaña. Las activas crean efectos fuera de las redes propias.

El 10 de marzo de 2015, el Centro para Estudios Estratégicos e Internacionales, junto con la unidad de seguridad cibernética del Departamento de Justicia de los Estados Unidos, organizó, con un grupo de destacados profesionales de la seguridad cibernética del sector privado, una mesa redonda sobre un aspecto de defensa de la cibernética que algunos han llamado "ciber defensa activa"[339].

Del análisis de las conclusiones, se puede extraer que existen medidas, algunas legales y otras no, que son utilizadas por ciertas empresas para llevar a cabo las denominadas "Acciones de defensa cibernética" que comprenden toda la gama de las actividades realizadas con fines de defensa de la red, y que podrían caracterizarse como una serie de actividades que abarcan desde la recolección de inteligencia hasta aquellas acciones tomadas en respuesta a una amenaza cibernética que puede afectar a una red remota. Tales actividades incluyen una serie de herramientas y técnicas que intentan prevenir o disuadir una actividad cibernética maliciosa, hasta aquellas otras tomadas en respuesta a una ciber amenaza particular y actual. Entre ambos extremos señalaron dos especialmente:

1. La recolección de Ciberinteligencia que proporciona información sobre las herramientas, infraestructura, tácticas y procedimientos del adversario puede utilizarse para reparar futuros daños. También puede suministrar información acerca del tipo y cantidad de la información robada de una empresa, la cual será utilizada con el fin de llevar a cabo una evaluación de los daños. Asimismo, señalaron que la inteligencia cibernética puede llevarse a cabo mediante el control legal de la

338 Ibidem.

339 CIS/DOJ Active Cyber Defense Experts Roundtable, March 10, 2015; Disponible en: https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/05/18/CSIS%20Roundtable%205-18-15.pdf

infraestructura usada por los intrusos, como, por ejemplo, los denominados *"hop points"* (trayectos entre router y router) para almacenar datos exfiltrados; y

2. Acciones más agresivas de ciberdefensa - a veces llamadas *"hacking back"*.

A tal extremo ello parecería ser cierto y en el Washington Post se publicó un artículo denominado: "*Cyberattacks trigger talk of 'hacking back'*"[340] en el cual Craig Nakashima y Douglas señalan que, a pesar de ser una actividad prohibida, algunos bancos instalan los denominados "*beacon*" (señuelo) los cuales potencialmente pueden ser adjuntados a datos sensibles, haciendo que sea más fácil tanto seguir el camino de los datos robados como determinar el camino que siguió a través de Internet.

Los autores afirman, además, que:

> ...el mero hecho de hablar de ello dentro de los círculos de seguridad cibernética puede acelerar una conferencia acerca de los muchos riesgos que acarrea, empezando por el hecho de que la mayoría de las formas de hackeo hacia atrás [N del A: o reversa] son ilegales y terminando con advertencias de represalias que podrían provocar una guerra cibernética a gran escala, con daños colaterales a través de Internet.

Las operaciones en el espacio cibernético y las fases de la campaña

Como ya se ha visto, la aparición del espacio cibernético introdujo nuevas formas de conflicto, y agregó nuevos niveles de complejidad en las operaciones y tácticas militares. En la actualidad, las operaciones en el espacio cibernético que ejecutan las fuerzas armadas (y, a menudo, las agencias de inteligencia, de seguridad y policiales) se llevan a cabo en todos los tipos de contienda durante todas las fases de las operaciones militares y en todos los niveles de la guerra.

Es sabido que, durante la campaña, los comandantes de componente deben asumir roles de fuerza a ser apoyada o de fuerza en apoyo durante todas las fases de esta. Para el General Williams[341]:

> ...aquellos familiarizados con las operaciones ofensivas en el contexto de los conflictos más recientes pueden llegar a inferir que la gran utilidad de las operaciones cibernéticas puede yacer en las dos primeras – alistamiento y movilización – a los fines de apoyar las operaciones de información, de engaño y de preparación territorial. Sin embargo, aun cuando ello sea cierto, en el futuro dichas operaciones producirán significativos efectos a lo largo de toda la campaña.

---

340 Craig, Nakashima, Ellen and Douglas-Gabriel, Danielle, Cyber attacks trigger talk of 'hacking back' Timberg, The Washington Post, October 9, 2014; Disponible en: https://www.washingtonpost.com/business/technology/cyberattacks-trigger-talk-of-hacking-back/2014/10/09/6f0b7a24-4f02-11e4-8c24-487e92bc997b_story.html

341 Williams, Brett T., The Joint Force Commander's Guide to Cyberspace Operations, Joint Force Quarterly 73 | April 01, 2014

Lo que ocurre es que la defensa pasiva requiere determinar ciertas capacidades cibernéticas del oponente, y eso se obtiene enlazando las propias vulnerabilidades con las del enemigo. Este proceso va a permitir identificar puntos decisivos cibernéticos, para disponer de la herramienta cibernética adecuada. Este es un proceso que lleva tiempo, porque hay que esperar que se definan las fases operacionales antes de conocer los requerimientos cibernéticos de protección de los sistemas de comando y control. Al igual que con el apoyo logístico, no se puede preparar hasta que no se conozca el plan de maniobra.

Otro nivel de complejidad de la defensa cibernética pasiva es establecer con claridad las capacidades cibernéticas del enemigo y sus intenciones operacionales con las vulnerabilidades propias y del enemigo conocidas. Para ello, es necesario "husmear", recorrer las redes y esta actividad se puede detectar. También la defensa pasiva requerirá conformar bases de datos y patrones de conducta y esto demanda tiempo y preparación.

A ello debe agregarse la necesidad de constituir los equipos cibernéticos propios para afrontar las exigencias cibernéticas previsibles y entrenarlos y, finalmente, coordinar con las numerosas autoridades involucradas a través de múltiples redes, sistemas, aplicaciones y Fuerzas Armadas, lo cual es una tarea de gran magnitud.

La defensa activa por su parte necesita de Reglas de Empeñamiento, autoridad para aplicarlas, y supone ciertas limitaciones de orden político. Tiene por tarea principal "eliminar al arquero" antes que la flecha llegue a impactar, aunque tiene la dificultad adicional en la selección de blancos cibernéticos, dada la rapidez del cambio de su naturaleza, su abundancia -porque cada uno requiere de una herramienta cibernética diferente-, la incapacidad para definir cuáles son efectos cibernéticos aceptables y cuáles son los inaceptables, y los daños colaterales no esperados que se puede causar.

La defensa activa puede incluir una serie de acciones, tales como exploración de datos, contra-vigilancia, infiltración de comunicaciones, gestión de crisis, análisis de datos masivos, rastreo de *bitcoin*, monitoreo de e-mails, búsqueda por palabras clave, lingüística, análisis predictivo, cálculo de riesgo, investigación del terrorismo, búsqueda de vulnerabilidades informáticas, o vigilancia de sitios. Se deben archivar contenidos y hacer seguimientos. Hay que ser cuidadoso con ciertas actividades de defensa activa, por dos razones: la primera de ellas es que muchas de estas acciones podrían ser ilegales, porque según sea la intención con que se hagan, pueden implicar la comisión de un delito. Si, por ejemplo, hay datos que apuntan a un terrorista potencial, pero se obtuvieron ilegalmente, las autoridades difícilmente conseguirían una orden judicial para, por ejemplo, golpear a la puerta de esa persona. Si la amenaza fuera lo suficientemente seria se apresurarían a conseguir una orden para investigar más; pero para que sea efectiva, la inteligencia rápida aceptable en una Corte se tiene que obtener legalmente.

La segunda razón es que, si es detectada, alerta sobre una capacidad que puede ser eliminada con rapidez. Por ejemplo, el *hacking back* es un contraataque digital contra los atacantes cibernéticos, con objetivos y métodos que van desde la recolección de evidencias para identificar a los perpetradores, la invasión de sus sistemas para borrar o recuperar datos, hasta medidas más severas como deshabilitar sus sistemas enteramente.

Pero, así como la ley advierte que perseguir a un ladrón no se considera defensa propia, o que tomar represalias contra una banda criminal en el mundo físico no debe hacerse, naturalmente el *hacking back* es ilegal y punible.

El derecho internacional aplicable a las operaciones cibernéticas

Como sucede habitualmente, los adelantos tecnológicos y sus consecuencias generan normas del derecho después que han ocurrido. La Guerra Cibernética no es la excepción. Una de las tendencias persistentes en la relación entre guerra y derecho es que cuando la sociedad en general se involucra en un nuevo ambiente, el derecho tiene que ponerse al día con la tecnología. Eso no debe sorprender: nadie escribe derecho para algo que no existe. Lo contrario sería algo así como pretender escribir el derecho del mar antes de que se inventasen los buques, o que se escribiese el derecho del aire antes que se inventasen los aeroplanos.

En 2009, el Centro de Excelencia de Ciber defensa Cooperativa de la OTAN (OTAN CCDCOE) una organización militar internacional con sede en Tallin, Estonia, acreditada por la OTAN en 2008 como un "Centro de Excelencia", invitó a un grupo de expertos internacionales independientes para producir un manual sobre la ley que debía regir la guerra cibernética de manera similar a lo ocurrido cuando el Instituto de Derecho Internacional Humanitario elaboró el "Manual de San Remo sobre derecho internacional aplicable a conflictos armados en el mar". El documento se denominó "*Manual Tallin 1.0 sobre el derecho internacional aplicable a la guerra cibernética*".

El enfoque del Manual original de Tallin fue sobre las operaciones cibernéticas más graves, aquellas que violan la prohibición del uso de la fuerza en las relaciones internacionales, sobre el derecho de los estados a ejercer su derecho de legítima defensa, durante el conflicto armado. Esta versión detallaba algunas reglas respecto del *jus ad bellum* y del *jus in bello* pertinentes a la guerra cibernética[342]. En ella[343], se establece que "un ataque cibernético es una operación cibernética, ya sea ofensiva o defensiva, que razonablemente se espera que cause lesiones o muerte a personas o daños o destrucción de objetos" y que, para los propósitos del Manual, dicha definición es de igual aplicación tanto en los conflictos internacionales como no internacionales.

En 2016, se editó el "*Tallin Manual 2.0 sobre el derecho internacional aplicable a las operaciones cibernéticas*"[344] que añade un análisis jurídico sobre los incidentes cibernéticos más comunes que ocurren diariamente y que son inferiores a los umbrales de uso de la fuerza o conflicto armado. La versión 2.0 retomó donde la versión 1.0 había quedado y en ella se establecen determinados puntos de vista de los expertos respecto de qué derecho internacional es de aplicación a la actividad cibernética.

---

342 Deeks, Ashley; "Tallinn 2.0 and a Chinese View on the Tallinn Process" Disponible en: http://www.lawfareblog.com/tallinn-20-and-chinese-view-tallinn-process

343 Tallinn Manual on the International Law Applicable to Cyber Warfare, P. 92 de 215

344 Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, Cambridge University Press (© from Cambridge University Press (© Cambridge

Vinculado con la posible violación de la soberanía de los países, Ashley Deeks[345] aprecia que:

> Un reto para los expertos será lograr un consenso sobre qué tipos de actividades llevadas a cabo por un estado violan la soberanía de otro estado: ¿Qué nivel de daño, intrusión o alteración de los datos es suficiente como para considerar que la soberanía de un país ha sido violada?

Según Deeks, en dicha conferencia y a título personal, el Profesor Huang ZhiXiong, (un profesor de la University de Wuhan), efectuó algunos comentarios sobre la sección del *jus ad bellum* del Tallinn 1.0. ZhiXiong observó que los parámetros para evaluar cuándo una actividad cibernética se considera como un uso de la fuerza (que incluye la gravedad, la directividad[346] y la invasividad [347]) eran muy flexibles y que, por tal razón, deberían ser más altos. En segundo lugar, solicitó un nivel más alto del que establece Tallin 1.0 respecto de cuándo un estado puede invocar el derecho de autodefensa. En su opinión, un estado no tiene derecho a la legítima defensa contra los ataques llevados a cabo por agentes no estatales, ni tampoco contra un ataque inminente.

Tal como señala Deeks, estas diferencias en las apreciaciones:

> ...se deberían a matices lingüísticos, pues en su opinión, seguramente China no cree que deba sufrir un ataque antes de tener derecho a responder, y seguramente China al menos contemplaría el uso de la fuerza militar para defenderse contra un ataque lanzado por un grupo bien organizado como el East Turkestan Islamic Movement desde la vecina Kazajstán.

Para Towsend[348],

> Tallinn 2.0 incorpora al Tallinn 1.0 publicado en 2013 pero, mientras que Tallin 1.0 intentó definir cómo el derecho internacional se relaciona con la ciberguerra, Tallin 2.0 amplía el contenido para incluir a la actividad cibernética que tiene lugar en la guerra real. Para reflejar esta expansión de contenido, ha cambiado el nombre de "aplicable a la guerra cibernética" a "aplicables a las operaciones cibernéticas".
>
> Tallinn 2.0, abarca un espectro completo del derecho internacional aplicable a las operaciones cibernéticas, desde los regímenes legales en tiempos de paz hasta la ley del conflicto armado, cubriendo una amplia gama de principios del derecho interna-

345 Deeks, Ashley, Tallinn 2.0 and a Chinese View on the Tallinn Process, Sunday, May 31, 2015; Disponible en: International Governance http://www.lawfareblog.com/tallinn-20-and-chinese-view-tallinn-process

346 Directividad: eufemismo por direccionalidad

347 Invasividad: eufemismo por capacidad de ser invasivo.

348 Townsend, Kevin, NATO Publishes Tallinn Manual 2.0 on International Law Applicable to Cyber Ops, February 03, 2017; Disponible en: http://www.securityweek.com/nato-publishes-tallinn-manual-20-international-law-applicable-cyber-ops

> cional y los regímenes que regulan los eventos en el ciberespacio. Algunos pertenecen al derecho internacional general, como el principio de soberanía y las diferentes bases para el ejercicio de la jurisdicción. Además, se examinan, en el contexto de las operaciones cibernéticas, numerosos regímenes especializados del derecho internacional, incluidos los derechos humanos, el derecho aeroespacial, el derecho del mar y el derecho diplomático y consular.

El denominado "Manual de Tallinn", recomienda un procedimiento a seguir por parte de los estados y las alianzas militares en caso de ataques masivos, pero no representa la opinión de ningún estado – nación. Su objetivo es exponer que las actuales normas legales internacionales (sobre todo en derecho internacional humanitario) son aplicables también en el espacio cibernético, lo cual significa que no son necesarias nuevas leyes. Sin embargo, Rusia y otros países consideran que la publicación de este documento constituye un paso hacia la legitimación del propio concepto de las guerras cibernéticas.

No son pocos quienes sostienen que lo que se llama "ataques cibernéticos" son realmente casos de espionaje, permitidos por el derecho internacional, o simplemente delitos, y que, por lo tanto, no están comprendidos dentro de las misiones de las fuerzas armadas. No hay acuerdo de definiciones al respecto.

Michael Schmitt, el experto en derecho internacional de los conflictos armados que dirigió el proceso de redacción del Manual Tallin, en una entrevista que le efectuara Kevin Townsend[349] señala que Tallin 2.0 amplía el análisis legal más allá de la guerra cibernética y estudia ciertas situaciones que se suceden en el ambiente civil como, por ejemplo, las intrusiones cibernéticas que enfrentan las organizaciones comerciales todos los días.

Para Schmitt, "hay un creciente entusiasmo por el derecho privado para que la industria contraataque a los agresores, como una extensión de la autodefensa, pero legalmente no pueden hacerlo". A propósito de ello da un ejemplo.

> Si una nación extranjera lanzó un ataque contra la Universidad de Exeter, habría un derecho de represalias; pero no por la Universidad de Exeter. El ataque podría ser considerado como un ataque contra el Reino Unido; y sólo el gobierno del Reino Unido podría responder.

A pesar de que el Manual Tallin 2.0 es útil en el derecho internacional aplicable a las operaciones cibernéticas, no establece ninguna nueva ley internacional ni representa la *opinio juris* de ningún Estado con respecto a las acciones que tomen o puedan tomar en el ciberespacio[350], aunque sí resulta un instrumento sumamente útil para quienes deban trabajar en estos temas.

---

349 Townsend, K., NATO Publishes Tallinn Manual 2.0 on International Law Applicable to Cyber Ops, Op. Cit.

350 Corn, Gary, Colonel, Tallinn Manual 2.0 – Advancing the Conversation. Disponible en: https://www.justsecurity.org/37812/tallinn-manual-2-0-advancing-conversation/

El Comandante del Teatro de Operaciones y las operaciones cibernéticas

El professor Richard M. Crowell[351] remarca que:

> Clausewitz sugiere la importancia de saber cómo librar una guerra sin los beneficios de la tecnología moderna y sistemas de comunicación. Entonces, ¿cómo debería prepararse un comandante operacional para la guerra en el siglo XXI? Sin duda, la habilidad de pensar operacionalmente "comienza con un entendimiento firme del arte operacional". En segundo lugar, un comandante debe estar preparado para luchar con poca o ninguna información fiable, ya que nuestros adversarios tienen la capacidad de degradar o denegar el acceso al espacio cibernético. Los futuros comandantes operacionales harían bien en prestar atención a las palabras de los coroneles Liang y Xiangsui: En guerra no existe ningún territorio que no pueda ser superado; no hay medios que no se puedan utilizar en la guerra; y no existe territorio y método que no se puedan utilizar de manera combinada.

Como se ha visto, la historia reciente demuestra que las operaciones en el espacio cibernético ocurren en diferentes tipos de operaciones militares y en distintos tipos de conflictos. Algunos podrían decir que la integración de las operaciones cibernéticas en el nivel operacional de la guerra no es apropiada. Piensan que los comandantes operacionales pueden lograr los objetivos militares con sus capacidades en el aire, la tierra, el mar y el espacio, y que evitar el empleo de operaciones cibernéticas ayudará a impedir que los conflictos escalen.

Más aún, desde el momento en que países como España, Brasil y Argentina, entre otros, crearon los Comandos/Mandos-Centros Conjuntos de Ciberdefensa, la mayoría de las discusiones respecto del empleo de las capacidades cibernéticas en una campaña coincidían en que el Comandante del Teatro era un simple abonado o requirente de requerimientos cibernéticos.

Ahora bien, ¿qué debería tener en cuenta el Comandante antes de decidir el empleo de las capacidades cibernéticas dentro del Teatro de Operaciones? La situación cambiaría si existiese un cuerpo de oficiales especialistas como comando de componente en un Teatro de Operaciones, o dado que se encuentra en el inicio de su creación, el Comandante del Teatro de Operaciones imparta orientación cibernética a cada uno de los Centros Cibernéticos de cada una de las fuerzas tradicionales.

En primera instancia debería tener presente que los objetivos operacionales siempre se encuentran en los dominios físicos del aire, el mar, la tierra y el espacio.

Para que un ataque a la red informática operacional funcione, un objetivo potencial tiene que ser accesible y tener vulnerabilidades que el atacante pueda encontrar útiles. Un comandante operacional no puede forzar su entrada en el espacio cibernético de un

---

351 Crowell, Richard M; War in the Information Age: A Primer for Cyberspace Operations in 21st Century Warfare; P. 20. Disponible en: www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA514490

enemigo. Los objetivos se limitarán a lo que el enemigo (o software) deje vulnerable. Incluso entre los objetivos vulnerables, puede ser difícil producir efectos en el ambiente físico. Aunque la tecnología del futuro pueda permitir operaciones en el espacio cibernético para obtener resultados físicos en los dominios clásicos, hasta la fecha ni un solo informe puede confirmar que un ataque a una red informática cause destrucción física. Una naturaleza restringida de operaciones de red de computadoras puede dar lugar a una extraordinaria cantidad de esfuerzo solo para encontrar un pequeño número de objetivos adecuados con muy pocas posibilidades de tener algún efecto sobre el medio ambiente físico.

Por otra parte, seguramente la infraestructura de la red de computadoras enemigas irá más allá del área de un comandante geográfico. De allí que resulte necesario disponer de un comando con alcance global para que la defensa cibernética se facilite. Por ejemplo, el *US Cyber Command* es un comando subordinado unificado bajo el *US Strategic Command* que está en mejor posición que un comando operacional unificado para asegurar que todas las fuerzas estadounidenses mantengan libertad de acción en el espacio cibernético.

También, el temor acerca del escalamiento apoya la noción de operaciones de redes de computadoras centralizadas bajo un comando conjunto de ciberdefensa que significa nivel de la estrategia militar, antes que en un comandante del nivel operacional. Existen pruebas de que los Estados Unidos evitaron atacar computadoras en red durante el ataque a Iraq por temor a escalar el conflicto al espacio cibernético. Un escenario en el cual un ataque cibernético de un comandante operacional que lleve al oponente a una represalia cibernética contra la infraestructura o el comercio del país, sería inaceptable. Para contener las ramificaciones de ataques a redes de computadoras, seguramente un Comando/Mando/Centro Conjunto de Ciberdefensa estará mejor posicionado que un Comandante Operacional.

Según Williams,[352] el proceso gradual de adopción de este nuevo ambiente va a hacer que el Comandante de Fuerzas Conjuntas tropiece con varias dificultades: la primera de ellas, es que el Comandante de Fuerzas Conjuntas no tendrá acceso a operadores del espacio cibernético con experiencia en los tres niveles, ya que inicialmente habrán sido entrenados en el nivel táctico y en la seguridad informática, pero carecerán de experiencia en las operaciones basadas en red, y en operaciones de información, y en los aspectos cibernéticos de un Plan de Campaña. La segunda dificultad es el nivel de seguridad que se le asigne a muchas operaciones en el espacio cibernético. Los niveles altos de seguridad pueden afectar el planeamiento integrado al ser compartimentadas las áreas de conocimientos del planeamiento y la ejecución de las operaciones. El tercer desafío es la autoridad delegada, donde la exigencia de reaccionar de inmediato se contrapone con cadenas de comando largas para decidir cuáles son las consecuencias deseables y no deseables de una acción militar en el espacio cibernético.

Este último dilema puede resolverse si se establece una única autoridad de ejecución por sobre el nivel del Comandante de Fuerzas Conjuntas. Esto implica la adopción de

352 Williams, Brett, The Joint Force Commander's Guide to Cyberspace Operations, Joint Forces Quarterly, 2nd Quarter 2014, Forum, P.18

un sistema de validación de blancos cibernéticos estandarizado y ejercitado previamente, establecimiento de ganancias y pérdidas técnicas como resultado de la operación cibernética, y riesgos que se presentan, lo cual implica que se deba establecer un procedimiento disciplinado de selección de blancos del mismo tipo que se realiza en los dominios convencionales.

No obstante, el espacio cibernético representa otro dominio en la guerra. Los ataques de computadores en red llevados a cabo aisladamente le dan al comandante operacional opciones muy limitadas pero su integración con las operaciones en otros dominios proporciona una multitud de opciones.

Los comandantes operacionales necesitan tener responsabilidad para defender las redes de computadoras propias porque si un enemigo tiene éxito en un ataque contra ellas, evitará que ese comandante operacional logre sus objetivos operacionales, de lo cual es el responsable.

El comandante operacional necesita entender las ramificaciones del ataque a las redes de computadoras en sus operaciones para saber la forma en que va a compensar en otros dominios los daños que sufra su infraestructura en el espacio cibernético. La idea de que las operaciones en el espacio cibernético pueden llevar al escalamiento descansa en la creencia de que uno puede controlar el uso de esa capacidad por parte del enemigo. Si un adversario posee la capacidad de atacar a computadoras en red, solo él decidirá si usará esa capacidad. El conflicto tomado como un todo influirá en la decisión del enemigo mucho más que cualquier decisión que un comandante pueda tomar en un dominio aislado.

Las cibercapacidades pueden ayudar al Comandante a alcanzar sus objetivos dentro de un plan de campaña coherente, integral, gradual y sincronizado, en el cual, el *tempo* operacional y la escala de operaciones cibernéticas se rijan por las condiciones que debe enfrentar el propio Comandante y no por las de los Comandos Conjuntos de Ciberdefensa. Ello no quiere decir que no deban o puedan trabajar de manera coordinada.

Sin un conocimiento holístico, global y acabado, como es el que tiene el Comandante del Teatro de Operaciones, las operaciones cibernéticas podrían verse afectadas debido a la falta de comprensión del entorno de las operaciones, por los efectos no deseados que pudieran llegar a causar, tanto en los neutrales como en el adversario y por su influencia en el cumplimiento de la misión del Comandante.

Si bien, y por lo general, existe una insuficiente legislación que autorice el empleo de las capacidades cibernéticas ofensivas en el nivel operacional y táctico, ello no implica que el comandante del Teatro no pueda consultar a los niveles superiores previo a ordenarlo. Para eso, debe tener en cuenta el impacto de sus acciones desde el punto de vista de la inteligencia, de las potenciales acciones cibernéticas y los problemas de capacidad y de control de los resultados, y las posibles consecuencias políticas que dichas acciones pudieran originar. Como ocurre en todo planeamiento, el comandante operacional debe comprender que siempre existirán restricciones políticas, legales y operacionales que limitarán el empleo de las capacidades cibernéticas.

Por ejemplo, en la Batalla de Midway, en abril de 1942, los estadounidenses habían descubierto la clave de cifrado de los japoneses, pero los comandantes que habían desci-

frado la clave recibieron órdenes de cuidar que los japoneses no se enterasen para hacerlos caer en una emboscada como fue Midway.

La capacidad de respuesta y efectividad de las operaciones cibernéticas deben contribuir a la unidad de esfuerzos y a la sinergia, cuando sea posible, con otras actividades en los ambientes aeroespacial, terrestre y marítimo dentro del Teatro de Operaciones, siempre de forma coherente con las políticas nacionales. El Comandante, además, debe tener capacidad para planificar y adaptarse a los cambios de dinámica y oportunidades en el entorno cibernético de un área de operaciones conjunta.

Conclusiones del Capítulo

La situación que se le puede presentar a un Comandante de Teatro de Operaciones será diferente según si el espacio cibernético se trata como un dominio diferente, o bien si se considera al componente cibernético como propio de cada uno de los componentes tradicionales.

La dependencia de los medios militares a las TIC las convierte en un objetivo de ciberataques. La amenaza es real debido a que hoy diversos estados y Ejércitos están llevando sus conflictos al espacio cibernético; de aquí que resulta fundamental asumir la necesidad de abordar la ciberdefensa en forma pasiva y activa, con el fin ulterior de tener una real capacidad cibernética de resiliencia, la que debe abarcar todas aquellas plataformas de redes y ordenadores consideradas como infraestructuras críticas en las fuerzas armadas. En consecuencia, resulta importante para las instituciones de la defensa asegurarse de que el acceso al espacio cibernético sea seguro y fiable.

La concientización del personal de cada Fuerza Armada es una tarea que debe ser llevada a cabo desde épocas de paz, sabiendo que las tareas de exploración cibernética son permanentes, y no se sabe con certeza quién es el que la está llevando a cabo. Puede ser desde agentes de un estado hasta un estudiante del colegio secundario, pasando por organizaciones no estatales delictivas.

La segunda tarea es detectar intrusiones, *sniffing*, y recorrido de redes. Estas son tareas de defensa pasiva y sus resultados deben ser puestos en conocimiento con premura en los otros usuarios de los otros componentes.

La tercera tarea es la de defensa activa, como el *hacking back* y dado que bordea la ilegalidad, debe ser autorizada por la Estrategia Militar. Esto ocurre también con las operaciones cibernéticas ofensivas, donde según sea el caso, la Estrategia Militar Cibernética podrá delegar inicialmente para Operaciones de Información.

En cuanto a lo atinente a las operaciones de red de computadoras, debe tenerse en cuenta que este concepto operacional es nuevo, no está totalmente desarrollado aún en los Estados Unidos y tiene por finalidad última que todos los elementos que las lleven a cabo estén en pleno conocimiento de la información disponible de manera de poder disponer el empleo de sus medios en forma rápida y oportuna. Tampoco es igual en los países occidentales que puedan llegar a conformar una alianza, pues la integración eventual, dada la necesaria velocidad de las operaciones, conectividad, efectividad y un proceso de toma de decisiones compartido, puede verse comprometida por tecnologías no estandarizadas y diferentes estructuras de comando.

La principal dificultad de un Comandante Conjunto en un Teatro de Operaciones será la de integrar el espacio cibernético dentro de los otros dominios tradicionales para poder así obtener los objetivos de la campaña. Si bien todo indica que la metodología empleada hasta el momento, con poca adaptación, sirve para las operaciones cibernéticas, el personal experto en cibernética que se incorpore al Estado Mayor de la fuerza conjunta debe reunir y poseer los requisitos y aptitudes indispensables para trabajar en operaciones aéreas, marítimas y terrestres.

Las operaciones cibernéticas de defensa pasiva deberían se conducidas por el Comandante que tenga autoridad sobre el ambiente de información a proteger. Las Operaciones de Defensa Activa pueden requerir autoridad delegada del nivel estratégico militar y esta autoridad delegada va a estar condicionada por la posibilidad de efectos no deseados producto de atacar nodos agresores, con la urgencia de tomar medidas defensivas para no perder el tempo operacional.

Las operaciones cibernéticas de defensa activas pueden estar dirigidas a un sinnúmero de blancos cibernéticos. Hasta hoy, solamente se ha usado *hackivismo* sobre páginas web con el propósito de confundir y hacer tomar decisiones equivocadas al enemigo. Eso va a crear incertidumbre en el adversario.

Los ataques cibernéticos llevados a cabo desde el ocurrido en Estonia en 2007 hasta el día de hoy han sentado precedentes que muchos países han seguido y tantos otros seguramente seguirán. Sumado a ello, la falta de regulación sobre el desarrollo de armas cibernéticas ha de conducir a su proliferación e incluso a que caigan en manos de estados hostiles, de organizaciones criminales e incluso de grupos terroristas.

Un ejemplo de ello lo constituye el ciberataque del 12 de mayo de 2017 el cual, según los expertos, el malware, se basó en un método que se cree fue desarrollado por la NSA como parte de su arsenal de armas cibernéticas. "El verano pasado, un grupo autodenominado los "*Shadow Brokers*" (corredores de la sombra) había publicado, en línea, herramientas digitales que había robado del arsenal de armas de *hacking* del gobierno de los Estados Unidos"[353].

En algunos casos, los ataques cibernéticos se han llevado a cabo dentro de los parámetros de las operaciones militares convencionales. En la actualidad, los soldados en el terreno dependen de enlaces de video y de datos cuando entran en combate. Como parte del proceso de preparación del campo de batalla, no hay nada que impida a los comandantes lanzar ataques preventivos contra las capacidades cibernéticas del adversario para asegurarse de que sus redes de datos no sean interrumpidas o atacar cibernéticamente las instalaciones de radar y de misiles de otro país antes de lanzar ataques aéreos contra ese país. Hay ocasiones en las que estas medidas son tomadas exclusivamente por el nivel de la Estrategia Militar para evitar escaladas incontrolables y represalias en el conflicto. Se deberá resolver caso por caso y en función del riesgo que se quiera tomar.

---

353 The New York Times, Scott, Mark, May, 13, 2017 "Hacking Attack has Security Experts Scrambling to Contain Fallout" Disponible en: https://www.nytimes.com/2017/05/13/world/asia/cyberattacks-online-security-.html?ribbon-ad-idx=2&rref=homepage&module=Ribbon&version=origin&region=Header&action=click&contentCollection=Home%20Page&pgtype=article

En otros casos, se han llevado a cabo operaciones ofensivas, independientemente de una operación convencional, de las cuales, el mejor ejemplo de un ataque de este tipo, lo constituye Stuxnet, el gusano informático utilizado para dañar las instalaciones nucleares en Irán.

También, estas operaciones cibernéticas ofensivas pueden utilizarse para obtener efectos que no fueran factibles de obtenerse por medios cinéticos, si bien, hasta hoy, este curso de acción no se ha empleado abiertamente. De adoptarse, la autoridad de planeamiento y ejecución debería estar en el nivel de la Estrategia General por las consecuencias que se pueden acarrear. Esa es la razón por la cual el Comandante del *US CyberCommand* es, a su vez, el *National Security Advisor* del presidente de los Estados Unidos.

El espacio cibernético es difícil de visualizar. Las operaciones cibernéticas deben ser articuladas con los otros componentes convencionales y, asimismo, con el nivel estratégico. Sin embargo, en la actualidad y con el nivel de conocimientos que se tiene, los métodos que se empleen para planificar y ejecutar operaciones convencionales son aptos también para el componente cibernético con mínimas adaptaciones sobre la forma de enunciar elementos de información, capacidades, vulnerabilidades y cursos de acción cibernéticos.

Lo que se ha escrito hasta aquí es pura elucubración teórica y la experiencia que se vaya adquiriendo dará lugar a nuevas iniciativas.

Habría que adaptar el marco legal para hacer posible las operaciones de defensa pasiva para bloquear agresiones, las operaciones de defensa activas para atacar nodos agresores, y las operaciones ofensivas para proyectar poder cibernético. Esto no se cumple solamente con capacidad para hackivismo, sino que requiere conocimientos informáticos avanzados.

Así también, deberían implementarse las medidas de seguridad informática en los tres componentes convencionales, bajo la dirección de la Estrategia Militar. Asimismo, a cada fuerza armada le correspondería iniciarse en las operaciones cibernéticas propias de su ambiente geográfico, sistemas de comando y control y sistemas de armas.

Todas estas medidas necesitan estar acompañadas por la capacitación de personal y que es fundamental que se realice progresivamente desde el nivel más bajo de simples operadores hasta la participación en operaciones de información y en los aspectos cibernéticos de una contingencia que pueda requerir un Plan de Campaña. Es en este nivel técnico donde deben desarrollarse sistemas operativos y programas de protección propios.

Las ventajas de usar armas cibernéticas son claras. Son más precisas que las bombas o misiles, y dañan más datos que instalaciones físicas, tienen muchas menos probabilidades de herir a civiles inocentes; aunque son armas nuevas y los críticos dicen que a su uso se le debe dar una cuidadosa consideración.

De todo lo anterior surge entonces que los Comandantes Operacionales de hoy deben prepararse para defender a la Nación en todos los dominios, lo cual incluye el espacio cibernético.

CAPÍTULO 5

LAS OPERACIONES CIBERNÉTICAS EN EL PLANEAMIENTO Y EJECUCIÓN DE LAS OPERACIONES MILITARES DE NIVEL OPERACIONAL

En este capítulo se analiza el empleo de las operaciones cibernéticas en el nivel operacional, recordando que este tipo de operaciones para países, como Brasil, se clasifican en operaciones de defensa, de explotación y de ataque, mientras que otros, como Estados Unidos, agregan vigilancia, inteligencia y reconocimiento y la preparación operacional del ciberespacio.

Para ello se dará respuesta a una serie de interrogantes tales como: ¿de qué manera las operaciones cibernéticas influyen en las operaciones militares?; ¿son de aplicación los principios de la guerra cinética a la guerra cibernética?; ¿cómo influyen en el nivel operacional y táctico las decisiones cibernéticas de los niveles superiores de dirección estratégica?; ¿cuáles deberían ser las coordinaciones con otros elementos del Estado nacional involucrados en el uso de la informática y las telecomunicaciones que pueden requerir posteriormente el empleo del componente armado del poder nacional?; ¿cómo pueden emplearse los medios cibernéticos en el nivel operacional tanto en lo que hace al planeamiento como a la ejecución de las operaciones?; ¿qué consideraciones corresponderían ser tenidas en cuenta para la ejecución de las operaciones cibernéticas ofensivas?; ¿qué debería contener el Anexo de Operaciones Cibernéticas del Plan de Campaña de un Teatro de Operaciones?; ¿cómo pueden las fuerzas conjuntas integrar las Operaciones en el Espacio cibernético para apoyar a las operaciones conjuntas?; ¿cuáles deberían ser los roles de cada uno de los Comandos de Componente en la guerra cibernética?

A partir de dicho estudio, se desarrolla el modo de incluir a las operaciones cibernéticas propiamente dichas en el proceso de planeamiento operacional. Asimismo, se trata de explicar holísticamente los complejos incidentes cibernéticos presentando enfoques preventivos y sistemáticos como elementos necesarios para un modelo/ensayo de diseño operacional.

Las operaciones cibernéticas en las operaciones militares

Como se ha podido apreciar, el espacio cibernético puede ser por un oponente para difundir propaganda, con fines de reclutamiento, para obtener financiación, para comunicarse entre sus miembros, para la planificación de sus operaciones y para la ejecución de operaciones de redes de computadoras. En estas operaciones de redes se pueden modificar sistemas algorítmicos automáticos a través de las ciberoperaciones, las cuales "*implican intencionalidad, voluntades contrapuestas y el enfrentamiento en el espacio cibernético con fines militares, elementos claves que permiten distinguir las ciberoperaciones de otras actividades como la seguridad informática o las operaciones de información*".[354]

El propósito común de las doctrinas militares en materia de ciberdefensa es alcanzar la superioridad informativa antes y durante el desarrollo de las acciones en el Teatro de Operaciones, reteniendo la libertad de acción en el espacio cibernético, proveyendo a los comandantes conjuntos de las adecuadas capacidades de Comando y Control al mismo tiempo que se previenen sorpresas estratégicas en el espacio cibernético. Significa que inicialmente al menos, el esfuerzo principal de esas doctrinas debe estar orientado a proporcionar, operar y defender la capacidad de comando y control (C^2) de las fuerzas propias.

Tal cual lo expresa el Major General J. Marcus Hicks, USAF[355],

> Cuando se consulta a los militares estadounidenses la mayoría dirá que "la defensa es el esfuerzo principal". En la práctica, sin embargo, la mayoría de las "ciber" discusiones se centrará sobre sofisticados hackers que llevan a cabo operaciones de ataque (sabotaje) o de explotación (espionaje).
>
> Como es bien sabido, a lo largo del último cuarto de siglo, las operaciones cibernéticas dentro de las operaciones militares se han incrementado, tanto en calidad como en cantidad. El bajo costo de los equipos informáticos permite que un adversario no tenga necesidad de fabricar armamento caro y sofisticado para suponer una amenaza significativa a las capacidades militares propias. Unos cuantos programadores pueden, si encuentran una vulnerabilidad a explotar, amenazar los sistemas logísticos, hurtar el planeamiento operacional, perturbar los sistemas de inteligencia y de comando y control, difundir información falsa o causar engorrosos problemas en la retaguardia.

Para Mathew Schwartz[356] "*los foros de delitos informáticos se han convertido en el dominio de empresas criminales bien organizadas y hasta algunos Estados - nación. La madurez económica que estos foros del mercado negro han alcanzado podría dar a los atacantes una ventaja sobre los aspirantes a defensores*".

---

354 Gómez Arriagada, Héctor; "Ciberoperaciones", Revismar 4/2013, P. 362, Disponible en: https://www.academia.edu/5087425/Ciberoperaciones.

355 Hicks, J. Marcus; A Theater-Level Perspective on Cyber; Joint Force Quarterly; 76, 1st Quarter 2015; P. 58

356 Schwartz, Mathew; Cybercrime Black Markets Grow Up; Diponible en: http://www.informationweek.com/cybercrime-black-markets-grow-up/d/d-id/1127911

El mercado negro del cibercrimen sigue existiendo y creciendo a un ritmo acelerado, consiguiendo continuamente productos más creativos e innovadores a pesar de que las operaciones defensivas se hacen más fuertes, las leyes se tornan más sofisticadas y nuevas tecnologías y conexiones aparecen en el mundo. Los productos pueden ser rápidamente modificados según los requisitos particulares y quienes los adquieren tienden a ser cada vez más especializados.

Los objetivos de los ataques cibernéticos varían según las causas y los estados finales deseados que los planificadores traten de alcanzar, y tal cual lo señalan Qiao y Wang[357], dos estrategas chinos: "El campo de batalla está a tu lado y el enemigo está en la red. Sólo que no hay ni olor a pólvora ni el hedor de la sangre".

Ante ello, la pregunta que cabría formularse es ¿qué efectos se pueden lograr a través del empleo de las operaciones cibernéticas en el nivel operacional?

Para las Fuerzas Armadas argentinas,

> ...las acciones militares pueden tener resultados o efectos estratégicos, operacionales o tácticos, basándose en su contribución para obtener objetivos estratégicos, operacionales o tácticos. Para que un efecto alcanzado sea considerado estratégico, operacional o táctico, el mismo debió haber sido planificado como tal en el nivel correspondiente[358].

Aunque esta definición persigue objetivos ordenadores en el ámbito académico, una distinción más certera es que los efectos estratégicos son los que afectan la dirección nacional o militar de las fuerzas del componente armado del poder nacional en su contribución a obtener el objetivo político; los efectos operacionales son los que afectan a las maniobras y a la logística preparatoria para los enfrentamientos; y los efectos tácticos son los que repercuten directamente en los enfrentamientos de las tropas.

Una conclusión inicial es que hay que comprender que en la guerra cibernética[359] carece de sentido una acción militar si esta no afecta a alguien o algo en el mundo físico. La naturaleza del objetivo en la guerra cibernética debe ser un componente físico, lógico o social que pueda verse afectado, positiva o negativamente, mediante el uso de computadoras interconectadas y de redes de datos.

En este caso, los efectos podrán variar desde operaciones contra el comando y control, operaciones sobre los datos para tomar decisiones, operaciones sobre los medios electrónicos que se usan, operaciones de disuasión, operaciones sobre la voluntad de

---

357 Liang, Q., & Xiangsui, W.; Unrestricted warfare; Beijing: PLA Literature and Arts Publishing House; 1999, P.129.

358 República Argentina. Ministerio de Defensa; Estado Mayor Conjunto de las Fuerzas Armadas; Planeamiento para la Acción Militar Conjunta Nivel Operacional, Proyecto 2015; Capítulo 1 P. 9

359 En esta investigación la definición de Guerra cibernética a la que se adhiere es la correspondiente a la de la Organización de las Naciones Unidas (según la Resolución 1113 adoptada por el Consejo de Seguridad de las Naciones Unidas el 5 de marzo de 2011) "...guerra cibernética significa el uso de computadoras o medios digitales por un gobierno o con el conocimiento explícito o la aprobación de ese gobierno contra otro Estado, o propiedad privada dentro de otro Estado incluyendo: El acceso intencional, interceptación de datos o daños a la infraestructura digital y a la infraestructura controlada digitalmente y la producción y distribución de dispositivos que pueden usarse para subvertir la actividad interna".

lucha; y en cuanto a los sistemas y redes, la interrupción o la disminución de la velocidad de acceso a los servicios y productos en línea, hasta la degradación y la destrucción de las operaciones de toda la red. El primero es más puramente una forma de guerra de la información, en la que el atacante se presenta con información que conduce a tomar decisiones erróneas y afecta a la mente de quienes deben tomar decisiones en el mundo físico. El último es análogo a la guerra cinética.

Algunos sistemas de armas combinan los sistemas de redes con las operaciones cinéticas. Por ejemplo, los sistemas de defensa antiaérea son más eficaces cuando están conectados en red y normalmente todos los componentes individuales de dichas redes (radares, computadoras, misiles) dependen de un software para que la operación resulte eficiente. Interferir esas redes o dicho software haría que esos sistemas sean menos eficaces. Lo mismo ocurre con la logística. Interferir las redes de logística podría resultar en envíos cancelados o insumos enviados a lugares equivocados. Los comandantes dependen de un flujo de información de sensores y recursos de inteligencia para determinar la ubicación, el movimiento y las intenciones del adversario. Si se interrumpiera dicho flujo, o se introdujeran inexactitudes deliberadas ello podría tener un efecto paralizante, aumentaría la probabilidad de que se cometiesen errores tácticos, que las tropas fuesen enviadas a una dirección incorrecta, que se produzca fratricidio o que sean conducidas a una emboscada.

Es por ello que, para Roy John Virden[360]

> Los efectos de cualquier ataque pueden agruparse en uno o más dentro de los tres tipos básicos que son: confidencialidad, integridad y disponibilidad. Un ataque contra el secreto o confidencialidad de un sistema de información puede provenir de muchos métodos comunes de ataque a las redes de computadoras y generalmente consiste en una intrusión no autorizada. Los ataques de este tipo incluyen software malicioso instalado localmente en una computadora, el acceso a una red desde un equipo remoto, o incluso la explotación de componentes inalámbricos como un ordenador portátil, una impresora o un asistente de datos personales[361]. El obvio peligro de un ataque secreto es que el enemigo puede llegar a conocer planes operativos y de inteligencia y luego atacar de manera adecuada. La integridad o exactitud de los sistemas de sensores militares, de inteligencia y sistemas de designación de blancos, puede ser afectada, mediante un ataque cibernético que altere maliciosamente la información de las bases de datos, lo cual puede desbaratar los esfuerzos de planificación y reducir la eficacia de los datos de los fuegos operacionales. Un ataque contra la disponibilidad, o denegación de servicio, puede interrumpir, degradar o detener completamente los sistemas militares lo cual posiblemente resul-

360 Virden, Roy John; Critical Vulnerability: Defending the Decisive Point of United States Computer Networked Information Systems; Naval War College; Disponible en: http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA415365

361 El asistente de datos personales, que se utiliza para determinados dispositivos como el Android es una aplicación, completamente personalizable, que espera órdenes, responde preguntas, realiza tareas, notifica eventos importantes, haciendo más fácil la rutina diaria.

te en una capacidad reducida para realizar funciones de C^2, retraso en las transferencias logísticas o soluciones erróneas de control tiro.

Debe tenerse en cuenta que, si bien muchas veces los efectos de algunos ataques cibernéticos pueden ser literalmente visibles desde el espacio, como un apagón eléctrico masivo en una ciudad, otros efectos pueden ser invisibles. Tal el caso de introducir información falsa o dificultar el flujo de datos de inteligencia sobre una red, pues su efectividad depende tanto de las reacciones de los seres humanos que la utilizan como de los datos técnicos. Por otra parte, un virus informático puede propagarse más allá de su objetivo y dañar partes neutrales, incluso a las fuerzas propias, o el oponente puede aislar el código que lo atacó, analizarlo, copiarlo y reinsertarlo de nuevo como si fuese propio. Por ello, la respuesta a un ataque o posible ataque, debe ejecutarse luego de identificar al atacante de manera oportuna[362], lo cual no siempre es posible, y considerar que los elementos de la respuesta incluyan la aplicación de opciones flexibles de disuasión.

Ello no resulta fácil de lograr, porque muchas veces se obtienen resultados diferentes a los que se intentaban. Para militares estadounidenses como Fink, Jordan y Wells[363]:

> El primer paso para atacar un objetivo con las operaciones cibernéticas ofensivas es ganar acceso al mismo. Sin acceso físico o electrónico al blanco, resulta imposible proceder con ellas. Por lo regular, un sistema vinculado a Internet, es más accesible, aunque entrar a las partes específicas puede ser difícil debido a su propio ambiente de seguridad de red. Un sistema cerrado, como el programa nuclear iraní, requeriría acceso privilegiado para obtener conocimiento de primera mano del ambiente informático en la instalación del blanco. Una vez que las fuerzas ganen acceso a un blanco, necesitan mantenerlo siempre y cuando deseen atacarlo. Las actualizaciones llevadas a cabo en la red o cambios de sistema en el mantenimiento regular del blanco, podrían dificultar mantener o recuperar el acceso. El riesgo de tener acceso a un sistema es que un adversario podría detectar la piratería informática mucho antes del ataque. El adversario descubriría qué sistemas fueron atacados. Por otra parte, el descubrimiento, sin duda alguna, podría ocasionar que se perdiera el acceso y la posibilidad de que el adversario analice el ataque para comprender las operaciones ciberespaciales estadounidenses y desarrollar mejores defensas o, hasta contraataques.

Por lo general, un ataque comprende tres etapas: la primera, que consiste en el reconocimiento y la enunciación. Durante del reconocimiento, el atacante intenta reunir información sobre la red para después, de manera confidencial, tratar de descubrir las vulnerabilidades del sistema en la fase de enunciación. La segunda etapa es la intrusión

---

362 También es cierto que existen operaciones secretas o encubiertas destinadas a engañar a un adversario haciéndole creer que son responsabilidad de otros grupos o Estados que no precisamente son los que planificaron e implementaron las operaciones.

363 Fink, Kallie D; Jordan John y Wells James E "Consideraciones para las ciberespaciales ofensivas"; Mayo-agosto 2014; Military Review en español; P. 24. (Fink es Capitán de Corbeta de las Armada de los EE.UU., Jordan, Mayor del Cuerpo de la Infantería de Marina y Wells, también Mayor aunque de la Fuerza Aérea de los EE.UU)

y el ataque, que es cuando el atacante aprende acerca de las vulnerabilidades del sistema y penetra en las redes. La inserción del *malware* y su explotación para obtener el propósito deseado es la última fase del proceso.

Sin embargo, el tema es tan nuevo que los académicos no coinciden ni siquiera en estas etapas. Para Joe Sarno, de Express Computers[364], las fases de un ataque cibernético son siete, a saber: *reconocimiento, búsqueda del arma cibernética más conveniente, entrega, aprovechamiento, comando y control, reconocimiento interno, mantenimiento y borrado de rastros.*

Es importante conocer las fases de un ataque cibernético para poder prevenir y anticipar contramedidas. Sabiendo la forma en que se ataca, es más fácil deducir las medidas contraofensivas de defensa pasiva.

En la fase **reconocimiento**, el atacante intenta obtener y comprender la organización y sus redes. Algunos sitios web que se usen pueden no ser seguros, ya que algunos operadores los pueden utilizar para distraerse o tomar un descanso. El atacante va a vigilar el contenido con herramientas proxy. Estos sitios web son investigados e identificados por los hackers cibernéticos cuando inserten un malware en esos sitios que son legítimos. También es importante llevar un registro de vendedores y tener en cuenta los niveles de acceso acordados. Habrá que construir una plantilla con preguntas clave y considerandos para evaluar la seguridad de cualquier tercero y, así, determinar los accesos de requerimientos mínimos.

En la segunda fase, la de la s**elección del arma**, es en la que el atacante a veces construye un código malicioso para explotar las vulnerabilidades que haya encontrado. Quien defiende tiene que tener una idea sobre cuál es el tipo de ataque que probablemente sea lanzado. Este ataque contra una aplicación o sistema que tiene como objetivo la ejecución de un código malicioso gracias al conocimiento de vulnerabilidades desconocidas hasta por el fabricante es el arma informática más peligrosa. Existen organizaciones que dan a conocer vulnerabilidades *0-day*, y que son las que dan origen a los parches de seguridad de los sistemas operativos. Un buen procedimiento de defensa pasiva es segmentar o dividir la arquitectura del propio sistema para minimizar el impacto de un quiebre potencial. La clave contra la amenaza *0-day* es la detección temprana. Si la amenaza proviene de delincuentes cibernéticos, habrá que concentrar los esfuerzos en desarrollar un programa de administración de vulnerabilidades y parches de seguridad. Si el sistema o la administración del sistema llevan a cabo consistentemente los parches sobre las vulnerabilidades conocidas, se incrementará la posibilidad de que los delincuentes pongan en riesgo la red. En la búsqueda de tecnologías de vulnerabilidades y parches, habrá que asegurarse que las soluciones puedan identificar todos los activos, los sistemas operativos y las aplicaciones.

La tercera fase es la **entrega o el depósito del malware en el sistema.** Una amenaza puede provenir tanto desde dentro como desde fuera de la organización, y puede ser intencional o accidental. Por lo tanto, hay que poner un esquema abarcador de programas y procesos para identificar los riesgos y las amenazas reales. El método por correo

364 Varney Rashi, Sarno Joe, The 7 phases of cyber attacks: 11de enero de 2017. Disponible en: http://computer.expressbpd.com/interviews/the-7-phases-of-cyber-attacks-joe-sarno-fortinet/20260/

electrónico de *phishing* es el más común para depositar malware. Hay que implementar cursos para los empleados alertándolos sobre el *phishing*, para que estén alertados sobre la sofisticación del ataque. Los empleados deben tener en sus computadoras tecnologías de seguridad para correos electrónicos para poder identificar y eliminar adjuntos maliciosos. Las soluciones que incluyan herramientas *sandbox*[365] son especialmente importantes porque pueden detectar malware que no haya sido detectado antes. Para las redes militares, es vital que en una misma computadora no se encuentren las placas de red, las placas de Internet y las placas de intranet. Deben estar en computadoras separadas, por razones de seguridad. Además, debe estar estrictamente prohibido el uso de drive USB, o drives de música como mp3 o mp4.

La cuarta fase es la **explotación del malware instalado**. Muchas de estas explotaciones ocurren mediante un ataque de phishing, por lo que es muy importante un administrador de parches. Hay que adoptar un solo navegador para la red, y asegurarse que tenga los últimos parches de seguridad, que se lo revise con regularidad, y se limite el uso de *plugs-in*[366] como Java o Flash. Al respecto siguen siendo útiles las *sandbox*.

La quinta fase es la de **comando y control**. Para defenderse en esta etapa, es conveniente inspeccionar el perímetro de la aplicación en uso, para detectar si el malware está pasando datos a su origen. Estas comunicaciones maliciosas normalmente van por medio de otros protocolos. Las inspecciones SSL para detectar violaciones a los protocolos de seguridad son los que mejor sirven porque pueden interceptar, abrir, inspeccionar y luego pasar tráfico encriptado una vez que se aprecie limpio. Una buena forma es usar una combinación de control, bases de datos confiables y filtros de URL para observar, inspeccionar y asegurar el tráfico.

La fase 6 se denomina **reconocimiento interno,** consiste en la preparación de los operadores para esta circunstancia. Lo normal que ocurre es que la gente entra en pánico y, para evitarlo, hay que tener planes ensayados y practicados. Si la red ha sido segmentada previamente en zonas, ya es una garantía, aunque el atacante haya eludido la capa de protección. La segmentación trabajará como puntos de control para aislar la intrusión. Probablemente, si la amenaza eludió las defensas, no habrá firma de software capaz de detectarla. Una de las maneras más prácticas de detectar la intensidad extraña de datos es monitoreando las capas 3 y 4 (red y transporte) de la pila OSI[367].

Finalmente, la fase 7 **mantenimiento** resulta de la intención de todo visitante malicioso de permanecer el mayor tiempo posible en tanto no sea detectado. Habrá que asegurarse que los servidores con información sensible no estén conectados a Internet. Esto va a ser la tarea de exflitración de datos sumamente difícil, por lo que hay que iden-

---

365 Sandbox es un sistema informático de aislamiento de procesos.

366 En informática, un complemento o plug-in es una aplicación o programa informático que se relaciona con otro para agregarle una función nueva y generalmente muy específica. Esta aplicación adicional es ejecutada por la aplicación principal e interactúan por medio de una interfaz de programación de aplicaciones. Complemento y plug-in se diferencian en que los plug-in son desarrollados por empresas reconocidas y tienen certificado de seguridad y los complementos pueden ser desarrollados por cualquiera.

367 El Modelo OSI (en inglés, Open System Interconnection) divide en 7 capas el proceso de transmisión de la información entre equipo informáticos, donde cada capa se encarga de ejecutar una determinada parte del proceso global.

tificar con anticipación todos los caminos de salida y monitorearlos. Habrá que poner atención especial a los servidores que tienen acceso a Internet.

Dicho en otras palabras, las operaciones cibernéticas deberán permitir explorar las redes del oponente, infectar sus sistemas de comando y control, al mismo tiempo que proteger a las propias redes de las posibles incursiones del oponente, y borrar los rastros de la incursión.

Ello no quiere decir que las etapas sean consecutivas e ininterrumpidas. Uno de los más sofisticados ataques cibernéticos, "*Red October*" se llevó a cabo en 2013, contra embajadas, centros de investigación nuclear, institutos de gas y petróleo y agencias gubernamentales en varios países. Según el informe de Kaspersky Lab, "Octubre Rojo" llamado también "Rocra" fue un ataque cibernético avanzado que había permanecido cinco años en los sistemas, antes de ser dirigido a las agencias de gobierno[368]. *"El principal objetivo de los atacantes era reunir documentos sensibles de las organizaciones comprometidas, que incluían inteligencia geopolítica, credenciales para acceder a sistemas informáticos clasificados y datos de dispositivos móviles personales y equipos de red"*[369].

Por último, merece destacarse que tanto en la doctrina de Brasil, como la de los Estados Unidos o la del Reino Unido, se establece que las operaciones que se lleven a cabo en el espacio cibernético deben ser consideradas como un complemento de las operaciones militares tradicionales[370], pues al mismo tiempo que pueden afectar la dirección, el planeamiento y la ejecución de las operaciones militares, también pueden producir efectos sobre los sistemas de comando y control de armas o sobre la población, a través del uso de la web con propósitos de propaganda y acción disuasoria o trasmitiendo información falsa.

Sin embargo, esto no es una fórmula, ya que en el conflicto Rusia Ucrania, las operaciones cibernéticas y las de Fuerzas Especiales Rusas tuvieron preeminencia sobre las operaciones convencionales. Las operaciones comenzaron en febrero de 2014 con el despliegue en Crimea de lo que Rusia ha dado en llamar *"polite men"* (hombre educado) (y los medios occidentales "*little green men*" "hombrecitos verdes") que son fuerzas especiales que no usan insignias. En apoyo a las operaciones de las fuerzas especiales, Rusia interfirió e interceptó las señales y las comunicaciones de Kiev, dificultando las operaciones ucranianas y aislando de manera efectiva la península de Crimea del ambiente de información[371].

---

368 Dave, Lee; "Red October' cyber-attack found by Russian researchers" Disponible en: http://www.bbc.com/news/technology-21013087.

369 Octubre Rojo tiene muchas similitudes con el virus Flame.

370 El 12 de abril de 2014, el destructor USS Donald Cook mientras navegaba en el Mar Negro fue sobrevolado por una aeronave rusa Su-24 que no transportaba bombas ni misiles, sino únicamente un contenedor con un sistema de guerra electrónica llamado Jibiny. El destructor está equipado con el sistema de combate de última generación Aegis, un sistema integrado que conecta entre sí los medios de defensa antimisiles de todos los buques en los que está instalado creando una red general que permite controlar y atacar cientos de objetivos al mismo tiempo. Al aproximarse al destructor, el sistema Jibiny del Su-24 puso fuera de servicio los radares, circuitos de control, sistemas de transmisión de información, etc. En otras palabras, todo el sistema Aegis quedó inutilizado. Después de esto, el Su-24 simuló un ataque con misiles contra el USS Donald Cook, repitiendo esa acción un total de 12 veces. Garamone, Jim; American Forces Press Service "Russian Aircraft Flies Near U.S. Navy Ship in Black Sea". Disponible en: http://www.defense.gov/news/newsarticle.aspx?id=122052

371 Pasi, Eronen. Russian Hybrid Warfare: How to Confront a New Challenge to the West, Washington, DC: Foundation for Defense of Democracies, June 6, 2016, P. 8 Disponible en: (http://www.defenddemocracy.org/content/uploads/documents/Russian_Hybrid_Warfare.pdf.

Estas operaciones convencionales fueron usadas únicamente como disuasión, pero como la población estaba ideológicamente ya separada, los efectos deseados se lograron con operaciones complementarias.

Según el General Williams[372],

> ...debido a la virtualidad del espacio cibernético, existe una tendencia a la centralización en el ápex estatal cibernético, pero se impone una libertad de acción al comandante de un Área de Operaciones Conjuntas para que con propios medios cibernéticos establezca su propio comando y control cibernético para las operaciones que se desarrollen en su propio territorio.

Para eso se le deben asignar medios cibernéticos, al igual que se hace con los tres componentes territoriales que no pierden su enlace con los Comandos de Componentes fuera del Área de Operaciones, sino que reciben su apoyo. En este punto tiene importancia haber trabajado anteriormente con la estrategia militar en la estandarización e interoperabilidad de los equipos de informática y comunicaciones del nivel operacional y superiores.

Probablemente, la transición en el conocimiento demande inicialmente que hoy un Comandante de Fuerzas Conjuntas, debido a su falta de experiencia, delegue, en principio, sus responsabilidades cibernéticas a especialistas en comunicaciones, inteligencia o en guerra electrónica. Este personal tiene importancia en las operaciones del espacio cibernético, pero la responsabilidad última siempre será del Comandante de Operaciones Conjuntas.

Las operaciones cibernéticas y los niveles de la guerra[373]

La publicación PC 20-01[374] divide a la guerra en tres niveles - estratégico, operacional y táctico - como herramienta de análisis metodológico. Esta separación no es simplemente por comodidad organizativa. Es, más bien, un reconocimiento de que la guerra es un asunto complejo que requiere coordinación desde los niveles más altos de la formulación de políticas hasta los niveles básicos de ejecución.

Sin embargo, cuando se analizan determinados casos, pareciera que tal división no se cumpliese de manera exacta.

Dispositivos no tripulados fueron empleados por las fuerzas armadas israelíes durante la operación *Protective Edge*[375], desde la etapa inicial de colección preliminar de

---

372 Williams, Brett T.; Ten propositions regarding cyberspace operations; Joint Force Quarterly 61; 2° quarter 2011; P. 11.

373 En esta parte de la investigación solo se tratará de aquellas operaciones que el propio comandante de teatro planifique y ejecute, en apoyo de sus planes y no de aquellas que deba ejecutar mediante la inserción de fuerzas, debido a que solo podrían ser ejecutadas desde las cercanías del objetivo.

374 República Argentina. Estado Mayor Conjunto de las Fuerzas Armadas; PC 20-01 "Planeamiento para la Acción Militar Conjunta: Nivel Operacional" Proyecto 2017; P. 1

375 El 07 de julio de 2014, después de una serie de ataques con cohetes desde Gaza a Israel, las Fuerzas Armadas israelíes iniciaron la operación Protective Edge (borde protector). Al décimo día de la operación, después de continuos atentados terroristas en Israel desde tierra, aire y mar, las Fuerzas de Defensa de Israel comenzaron la fase de la operación en tierra.

> inteligencia de los blancos, cuando las fuerzas todavía no habían comenzado a operar, durante la etapa donde se prestó apoyo a la maniobra de la tierra, en los ataques contra los túneles subterráneos y en el lanzamiento de cohetes contra los bunkers y residencias de los terroristas. Los vehículos aéreos no tripulados funcionaron continuamente antes, durante y después de cada operación, en virtud de que constituyen un activo de inteligencia en tiempo real de alta calidad. Las capacidades incorporadas de este diseño, que es comandado por operadores en tierra y que es capaz de ejecutar extensas operaciones en el contexto de las diversas misiones, proporcionan los elementos de control operacional para controlar continuamente el Teatro de Operaciones de una manera flexible y adaptativa. Suficiente es escuchar el zumbido constante que acompaña a todos los videos filmados en la Franja de Gaza para entender la presencia permanente de vehículos aéreos no tripulados sobre el territorio y el efecto que tenían en el conocimiento del campo de batalla por parte del comandante.

Alon Unger[376], presidente y fundador de las Conferencias de Defensa de Israel de vehículos aéreos no tripulados plantea el siguiente interrogante ¿son los vehículos aéreos no tripulados un recurso táctico, destinado a apoyar el esfuerzo militar, o un recurso estratégico cuyo beneficios e implicancias trasciende el hecho de que sea un sistema de armas moderno? Para Unger, quien además sirvió en la Fuerza Aérea Israelí (IAF) como comandante en jefe con varias unidades operacionales de campo, así como en la sede de dicha fuerza, la respuesta es simple. Estos vehículos trabajan en el nivel de los enfrentamientos, por lo tanto, son del nivel táctico. Los efectos que causen van a variar según el nivel donde se obtengan, al mismo estilo de lo que ocurre con los bombardeos estratégicos de la fuerza aérea.

En un artículo que escribiera en 2014 el General Brett T. Williams[377] Director de Operaciones, J-3, del *United States Cyber Command* expresó: "Necesitamos una teoría para las operaciones del espacio cibernético que nos permita entender las implicancias de emplear capacidades del espacio cibernético en los niveles táctico, operacionales y estratégicos".

A nuestro entender, las actividades cibernéticas ejecutadas por las fuerzas militares se llevan a cabo en todos los tipos de conflicto, durante todas las fases de las operaciones militares y en todos los niveles de la guerra.

Los ataques a un sistema informático en red son tan numerosos como tipos de sistemas existen y varían desde el acceso no autorizado hasta la destrucción física. Lo más importante que un comandante de nivel operacional debe comprender es cómo los efectos de estos ataques pueden influir en su capacidad para alcanzar las metas y objetivos, y que la naturaleza de los ciberataques es potencialmente de nivel estratégico, razón por la cual, cualquier ciberataque que ordene ejecutar es posible que tenga consecuencias no deseadas como, por ejemplo, generar riesgos políticos.

---

376 Unger, Alon; "UAVs - A Tactical Resource or a Strategic Asset?" En Israel Defense. Disponible en: http://www.israeldefense.co.il/en/content/uavs-tactical-resource-or-strategic-asset; El CV resumido del autor puede consultarse en: http://uvid2016.israeldefense.co.il/en/speakers

377 Williams, Brett T.; "The Joint Force Commander's Guide to Cyberspace Operations;" Joint Force Quarterly 73 (2nd Quarter 2014); P. 12–20.

Desde el punto de vista de Milan Vego[378]

Los nodos de comunicaciones no siempre deben ser atacados pues tal acción podría ser incompatible con los objetivos nacionales o podría ser política, diplomática, o psicológicamente imprudente o legalmente sospechosa. A nivel estratégico, no solo los elementos militares pueden ser engañados, destruidos o neutralizados, sino que también los elementos civiles de los sistemas de información del enemigo, tales como la banca, el comercio, el transporte y los medios de comunicación; ellos pueden formar parte del centro de gravedad estratégico.

Para Eric Schmitt y Thom Shanke[379],

Justo antes de los ataques encabezados por Estados Unidos contra Libia en marzo de 2011, la administración Obama debatió intensamente la manera de iniciar la misión con un nuevo tipo de guerra: una ciberofensiva destinada a interrumpir e incluso desactivar el sistema de defensa aérea del gobierno de Gadafi, que amenazaba a los aviones de combate aliados. Mientras que las técnicas exactas bajo consideración permanecen clasificadas, el objetivo habría sido romper el firewall de las redes de computadoras del gobierno libio para cortar los vínculos de comunicación militar y evitar que los radares de alerta temprana recopilaran información y la retransmitieran a las baterías de misiles. Sin embargo, los funcionarios de la administración e incluso algunos oficiales militares se opusieron, temiendo que podría sentarse un precedente para que otras naciones, en particular Rusia o China, pudieran llevar a cabo similares ofensivas y cuestionaron la posibilidad de llevar a cabo el ataque en tan corto plazo. También fueron capaces de definir si el Presidente tenía el poder de proceder con un ataque de ese tipo sin informar a Congreso. Finalmente, los funcionarios estadounidenses rechazaron la guerra cibernética y utilizaron las aeronaves convencionales, misiles de crucero y aviones teledirigidos para atacar los sistemas misilísticos de defensa aérea libios y los radares utilizados por el gobierno del coronel Muhammad Gadafi.

Cierto es que los actuales dispositivos cibernéticos ofrecen a los comandantes una capacidad para crear efectos a nivel operacional, en apoyo a una estrategia más amplia y complementan las capacidades existentes.

Maren Leed[380] efectúa una distinción que ayuda a aclarar otra de las diferencias entre los ciber objetivos estratégicos y los operacionales y tácticos.

---

378 Vego, Milan; Joint Operational Warfare: Theory and Practice; 20 September 2007; Reprint of 1st ed., 2009; P. IX - 111

379 Schmitt, Eric and Shanker, Thom; "U.S. Debated Cyberwarfare in Attack Plan on Libya"; artículo publicado en el New York Times, oct 17, 2011 Disponible en: http://www.nytimes.com/2011/10/18/world/africa/cyber-warfare-against-libya-was-debated-by-us.html?_r=1.

380 Leed, Maren; "Offensive Cyber Capabilities at the Operational Level: The Way Ahead" Center for Strategic and International Studies (CSIS), Disponible en: https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/130916_Leed_OffensiveCyberCapabilities_Web.pdf .

> Lo que sucede es que cuanto más "estratégicos" sean los objetivos, es decir, de los que se pueden esperar efectos más importantes sobre el adversario o que podrían resultar decisivos en el curso de conflicto, es más probable que estén conectados vía un cable. Se trata de grandes redes de mando y control nacionales y su infraestructura de apoyo. Estos objetivos suelen también ser relativamente fijos y probablemente bien defendidos en los dominios de la física y la cibernética. Pero los comandantes de menor nivel que tal vez deseen utilizar las cibercapacidades en un sentido más limitado (por ejemplo, para denegar las comunicaciones locales por un período limitado de tiempo, interrumpir un carril de maniobra cerrando las señales de tráfico en una porción de una ciudad, o suprimir un sistema de dirección de armas tácticas) pueden ser más propensos a buscar afectar a las redes inalámbricas[381] o blancos que dependen de una red local más circunscrita.

En el mundo sobran ejemplos de ataques cibernéticos de nivel estratégico militar mediante los cuales se habrían manipulado redes de energía eléctrica llevándolas a un *blackout*, como podría haber sido el que impactó a millones de brasileros en 2005 y 2007[382], o las que permitirían la apertura de las compuertas de represas o provocar accidentes de ferrocarril. Puede crearse un caos con la simple inserción de un troyano, a través de *malware* en un sistema militar de comando y control, comunicaciones, computadoras, inteligencia, vigilancia y reconocimiento (C4ISR) o en un sistema SCADA[383] de una empresa de energía eléctrica.

En el nivel operacional, para Parks y Duggan[384]:

> Existen ejemplos de ataques que han afectado tanto a quienes toman decisiones tácticas como estratégicas. Las primeras pueden estar relacionadas con el engaño respecto de la ubicación y el tamaño del enemigo y de las fuerzas amigas. En el nivel operacional, el tiempo de arribo y cantidad de suministros y refuerzos podría ser manipulado para provocar decisiones erróneas como, por ejemplo, atacar con escasa munición o retener un ataque por temor a la falta de suministros. Tampoco hay que

---

381 Para Thuente y Mithun Acharya: Es sabido que las interferencias y sus contramedidas tienen una larga historia en las operaciones militares. Inhibidores de nodos de relativo bajo costo pueden ser diseminados en el campo de batalla enemigo con el fin de generar ruido para "hacer caer" la red enemiga, perturbar redes de sensores, o incluso descomponer redes de comando y control. Cuanto más eficiente sea, más asegurarán su longevidad y se reducirá la probabilidad de su detección. Disponible en: http://networking.ncsu.edu/ThuenteMilcom06_FINAL.pdf.

382 The Huffington Post, Cyber Attacks Caused Brazil Power Outages, 18 marzo 2010. Disponible en: http://www.huffingtonpost.com/2009/11/07/cyber-attacks-caused-braz_n_349530.html.

383 Los sistemas conocidos como SCADA (Supervisory Control and Data Acquisition System) permiten el control de los procesos industriales en tiempo real utilizando computadoras y software para monitorear y controlar diferentes sistemas que incluyen desde las plantas de energía nuclear y las redes de distribución de las usinas eléctricas hasta playas de maniobras ferroviarias, instalaciones de tratamiento de agua potable y/o de desechos cloacales.

384 Parks, Raymond C.; Duggan, David P.; "Principles of Cyber-warfare" Proceedings of the 2001 IEEE Workshop on Information Assurance and Security United States Military Academy, West Point, NY, 5-6 June, 2001. Disponible en: http://opendawn.com/ewar/docs/dissertationsources/educationalsource2.pdf.

desechar, el caso de que quienes toman decisiones estratégicas puedan ser engañados por atribuir las acciones a otros países o grupos distintos al atacante real.

Sin embargo, dado que esta investigación trata de generar debates entre quienes deban planear operaciones o escribir doctrina, es que se ha tomado en consideración el punto de vista de Dombrowski y Demchak[385] quienes sostienen que:

Nuestra posición es nuevamente sencilla; el conflicto cibernético entra en juego en los tres niveles y los conecta interactiva y sistémicamente. A nivel estratégico, las políticas nacionales deben prever a los comandantes operacionales con los objetivos a lograr en el espacio cibernético (y a que ciberoperaciones deben contribuir) y los lineamientos respecto de cómo los ciber instrumentos pueden utilizarse consistentemente con la legislación nacional, así como los medios para adquirir y operar dichos instrumentos. En el nivel táctico, los comandantes deben pelear batallas utilizando no sólo medios cinéticos, sino que también instrumentos cibernéticos ofensivos y defensivos. Como la doctrina conjunta observa, los tres niveles se solapan durante la ejecución de una operación militar; por lo tanto, "los comandantes y su personal en todos los niveles deben anticipar cómo sus planes, operaciones y acciones pueden afectar a los otros niveles (los de arriba y los de abajo). El nivel operacional vincula la estrategia y táctica mediante el establecimiento de objetivos operacionales necesarios para alcanzar el estado final militar. Secuencia las acciones tácticas para lograr los objetivos estratégicos.

Además de ello, deberá tener siempre presente que las acciones cibernéticas ofensivas descentralizadas, es decir, las que se originan en el nivel operacional y que no lleva a cabo el Comando Conjunto de Ciberdefensa, deben ser viables técnicamente al igual que en caso de los fuegos operacionales, y ejecutadas de manera discreta, es decir, a la medida de una escala que, a través de la coordinación se ha considerado *aceptable* (por ejemplo, limitado a un objetivo individual o clase de objetivos); *oportuna*, que los objetivos son capaces de ser identificados, penetrados y atacados en plazos que son relevantes para los comandantes operacionales; y lo suficientemente preservadoras de las acciones de inteligencia que puedan estar llevándose a cabo.

Las acciones cibernéticas ofensivas deben encajar perfectamente en el ciclo de adquisición y localización de blancos pues muchas veces requerirán de cuantioso trabajo y tiempo adicional para incorporarlas en la planificación deliberada[386].

Finalmente, como señala Freedman[387],

Un ataque efectivo requiere de considerable inteligencia sobre la precisa configuración de los sistemas digitales del enemigo como así también de los puntos de entrada a sus redes. El posible anonimato y la sorpresa del ataque pueden tener sus atractivos,

---

385 Dombrowski, Peter; Demchak, Chris C.; Cyber War, Cybered Conflict, and the Maritime Domain; Naval War College Review; Volume 67, Number 2; 2014; P. 74

386 Fink, Kallie D; Jordan John;Wells James E "Consideraciones para las ciberespaciales ofensivas". Op.Cit

387 Freedman, Lawrence; "Strategy: A History"; Oxford University Press. Edition 2013; P. 229.

pero cualquier propósito de montar uno, deberá efectuar un análisis entre la posibilidad de éxito en el caso de que el enemigo esté alertado, el daño real que pueda llegar a causar el ataque, la velocidad de recuperación y la posibilidad de retaliación (la cual no necesariamente puede ser de la misma naturaleza que la del ataque).

Por todo ello, y porque existen aplicaciones cibernéticas adecuadas para todos los niveles de la guerra, es que deben ser desarrolladas, desplegadas y utilizadas, en la medida de lo posible. En este sentido, se adhiere a lo que señala Leed[388]:

> ...desde la perspectiva limitada de la naturaleza de cualquier "nodo" específico que podría ser objeto de un ataque cibernético particular, cualquier potencial objetivo teóricamente podría ser estratégico, operacional o táctico, según el propósito para el cual es utilizado y por quién. Dado que un determinado objetivo no puede ser atribuido *per se* a un "nivel de guerra" es importante examinar los tipos de efectos que desean crear los diversos escalones de comando, así como las condiciones bajo las cuales ellos pueden pretender empeñarse mediante el uso de la cibernética.

De conformidad con lo que afirma este autor[389]:

En todos los niveles, el objetivo de los ciberataques es negar, interrumpir o degradar las capacidades enemigas, directa o indirectamente (por ejemplo, a través del engaño). A nivel estratégico, los comandantes son más propensos a estar interesados en grandes nodos o con excesiva influencia en la mente de los potenciales adversarios. Un engaño o una interrupción temporal puede ser suficiente para determinar la acción del adversario, pero la destrucción también podría ser un objetivo. Casi por definición, estos objetivos se identifican por adelantado, a veces con años de trabajo preparatorio. Los comandantes de nivel táctico, por otra parte, son más proclives a emplear ataques cibernéticos como parte de sus actividades en apoyo de su esquema maniobra o de fuegos y enfrentarse a blancos fugaces que son difíciles de prever de antemano.

Asimismo, toda acción cibernética ya sea usada como operación de información o como ataque a redes que influya en forma anticipada sobre la maniobra y la logística preparatoria a los enfrentamientos es una operación cibernética del nivel operacional.

Así como los blancos en el nivel estratégico pueden incluir tanto infraestructuras civiles como hardware militar en el nivel operacional, el foco podría estar puesto en los sistemas integrados de defensa aérea del adversario o en el apoyo a los procesos de colección y análisis de inteligencia.

Las operaciones cibernéticas y los principios de la guerra

En lo que respecta a la conceptualización relativa a la seguridad y a la defensa, no debe olvidarse que muchas de las cuestiones que se presentan como los nuevos retos del siglo XXI son perfectamente identificables en conflictos del pasado y que los conceptos en desarrollo pueden ser novedosos en su denominación, pero no lo son tanto en su fondo.

388 Leed, Maren; Op. Cit.

389 Ibídem

Así, mucho antes de la "revolución en los asuntos militares" (entre estos la transformación de las fuerzas armadas, las operaciones basadas en efectos, el enfoque global de la seguridad, el combate en coalición, etc.) los responsables de la elaboración de la estrategia militar se plantearon cuestiones muy similares y lo hicieron apoyándose tanto en las lecciones aprendidas de conflictos anteriores como en la puesta en práctica de teorías que, en algunos casos, se remontan a más de 2.000 años de antigüedad, lo que hace aún más sorprendente su vigencia. En este sentido y, a pesar de que la moderna tecnología militar ha revolucionado la mayor parte de las dimensiones materiales de la guerra desde el siglo XIX, la lógica de los conflictos permanece básicamente inalterable. Esto explica por qué obras como "De la guerra" de Carl von Clausewitz y "El arte de la guerra" de Sun Tzu, permanecen como marcos conceptuales relevantes para el estudio de la política y la estrategia, incluso en estos días. Basta recordar que, Carl von Clausewitz describe a la guerra como *"un verdadero camaleón"*[390], que cambia permanentemente y adapta su apariencia a las variables condiciones sociopolíticas en las que se desarrolla.

Actualmente, es un hecho la incorporación del espacio cibernético para la ejecución de operaciones de Comando y Control y de Información, como un complemento de la guerra convencional pero, debido a que el espacio cibernético difiere de los otros dominios, han surgido distintas opiniones respecto de cuáles de los tradicionales principios de la guerra son de aplicación a la guerra cibernética o de qué manera los esfuerzos en el espacio cibernético pueden contribuir a la aplicación de los principios de la guerra en el campo de batalla. Asimismo, existen otras opiniones que sostienen que muchos de esos principios no son de aplicación o que se deben aplicar en forma diferente y, con ello, optimizar los factores operacionales de *tempo*, fuerza y espacio que todo comandante combina para lograr los objetivos militares.

La dirección, el planeamiento y la ejecución de la guerra están influenciados por una serie de preceptos amplios que se conocen como principios de la guerra. Estos principios, que han perdurado a pesar de los cambios de contexto y de la tecnología, forman parte conceptual de todas las doctrinas militares y guían en forma general todo el espectro del conflicto[391].

Si bien existen otros autores como Liddell Hart o Jomini que escribieron sobre ellos, podría decirse que existen dos visiones predominantes: la visión occidental de Clausewitz y la oriental vista por Sun Tzu. El mundo occidental de Clausewitz concibe la guerra entre estados, con la finalidad de alcanzar un objetivo político y, para ello, utiliza principalmente los principios de masa, objetivo y maniobra. El mundo oriental de Sun Tzu imagina la guerra centrándose en la importancia de la inteligencia, el engaño para derrotar la mente del enemigo y saber que las relaciones entre las cosas son más importantes en la estrategia de guerra. *"Obtener cien victorias en cien batallas no es el mérito máximo; sojuzgar al enemigo sin combatir es el mérito máximo"*[392].

---

390 von Clausewitz Carl (Autor) "On War", Indexed Edition; Editada y traducida por Michael Howard y Peter Paret; Princeton University Press; 1989; P. 89

391 Históricamente los principios de la guerra convencionales del Mariscal Foch se aplican a cada dominio por separado, y al campo de batalla en su conjunto.

392 Sun Tzu, "The art of War"; traducido por Samuel B. Griffith; Oxford University Express; 1963; P. 77

Para la doctrina argentina los principios de la guerra son: Objetivo, Moral, Ofensiva, Seguridad, Sorpresa, Concentración, Unidad de Comando (y de esfuerzo), Sostenibilidad, Maniobra, Simplicidad y Libertad de Acción[393]; no obstante, es necesario destacar que ellos no son universales pues responden a las propias realidades de los países e incluso tampoco lo son entre las fuerzas armadas de un mismo país, dadas las diferentes naturalezas de los escenarios en las que estas operan[394].

Cabe preguntarse entonces ¿cuáles de todos estos principios de la guerra y de las operaciones conjuntas serían de aplicación para las operaciones cibernéticas que puedan llevarse a cabo en el marco de una campaña?

Para responder a este interrogante, en esta parte de la obra se exponen las distintas posturas académicas respecto de la guerra cibernética y los principios de la guerra partiendo de la premisa de que si bien, y tal como lo considerara Clausewitz, la guerra es algo que sucede entre estados, con fronteras y límites establecidos, ello no necesariamente es así cuando se consideran las ciberoperaciones. Una intrusión o un ataque cibernético, como ya se ha mencionado varias veces a lo largo de este escrito, pueden o no ser patrocinados por un estado, ejecutarse desde cualquier lugar del mundo, o hasta incluso utilizar medios del espacio cibernético dentro del propio territorio (o de un tercer país).

Principio del objetivo

El principio del objetivo, es considerado el "*primus inter pares*" y su propósito es el de "*dirigir cada operación militar hacia un objetivo claro, definido, decisivo y alcanzable*"[395].

Robert Leonhard (en su libro, *The Principles of War for the Information Age*) argumenta que el principio del objetivo no es de aplicación a la guerra cibernética pues dicho principio se centra en la batalla decisiva. Además, dado que la naturaleza de la guerra cibernética es intrínsecamente continua y a menudo es difícil identificar una clara y decisiva "batalla" virtual, Leonhard sostiene que este principio, definido en la manera en que tradicionalmente se lo hace, no es de aplicación al dominio cibernético[396]. Sin embargo, si no existiese un objetivo para guiar las acciones de las fuerzas conjuntas, ¿cómo podrían saber los comandantes subordinados cuándo se han alcanzado los criterios de terminación?

Para Rivera[397]:

---

393 República Argentina. Ministerio de Defensa; Estado Mayor Conjunto de las Fuerzas Armadas; PC 00 – 01; Parte II; Doctrina Básica Militar Conjunta; Anexo 1 Los Principios de la Guerra; Público; Proyecto; 2014.

394 Brasil. Ministério Da Defesa do Brasil; Doutrina Militar de Defesa; MD51-M-04; 2007; P. 37/48.

395 Los propósitos de cada uno de los principios de la guerra que se enunciarán a lo largo del trabajo han sido extraídos de la publicación PC 00 – 01; Parte II; Doctrina Básica Militar Conjunta; Anexo 1 Los Principios de la Guerra; Público; Proyecto; 2014

396 Citado por Farmer, David B; Do the Principles of War Apply to Cyber War? School of Advanced Military Studies United States Army Command and General Staff College; Fort Leavenworth, Kansas; Disponible en: handle.dtic.mil/100.2/ADA522972

397 Rivera, Jason; A Theory of Cyberwarfare: Political and Military Objectives, Lines of Communication, and Targets; Georgetown's Security Studies Review; Disponible e:n http://georgetownsecuritystudiesreview.org/2014/06/10/a-theory-of-cyberwarfare-political-and-military-objectives-lines-of-communication-and-targets/.

Sería fácil asumir que la naturaleza del objetivo de las operaciones en el espacio cibernético son las fuerzas del adversario, sus fortalezas o guarniciones. Aquí es donde es importante entender las diferencias clave entre los dominios físicos (tierra, mar, aire y espacio) y el dominio de la cibernética. Una definición simple y concisa del espacio cibernético es un dominio caracterizado por la física, la lógica y la interconexión social de computadoras y redes de datos. Por lo tanto, la naturaleza del objetivo en la guerra cibernética debe ser un componente físico, lógico o social que pueda verse afectado, positiva o negativamente, mediante el uso de redes de computadoras y datos interconectados.

Independientemente de que la naturaleza del objetivo sea física (por donde se transmiten la información y los datos), lógica (es el primer punto donde se pierde la conexión con la dimensión física del entorno de información), social (un individuo o grupo de individuos conectados *online* que tienen importantes implicancias para la fuerza conjunta), o psicológica, lo concreto es que, sin un objetivo claro y alcanzable, la amenaza no puede ser evaluada adecuadamente, no se pueden desarrollar los cursos de acción y las consecuencias y contingencias no podrán ser identificadas. En el objetivo están enfocados todos los esfuerzos para alcanzar el estado final deseado, por lo que pareciera ser que es un principio que se mantiene incólume a pesar de los cambios de las últimas décadas. Definir con claridad un estado final posible sigue siendo crucial para las operaciones militares exitosas.

En algunos casos, las actividades en el espacio cibernético podrán lograr determinados efectos en el nivel operacional; por ejemplo, un ataque cibernético para abatir o corromper la red de computadoras del comando adversario puede tener repercusiones a través de todo el Teatro de Operaciones.

Lo concreto es que "...tanto el defensor como el atacante solo están en capacidad de controlar una parte muy pequeña del espacio cibernético que utilizan. Quien pueda controlar la parte del espacio cibernético que utiliza el adversario puede controlar al oponente"[398].

Principio de masa o concentración

Al sincronizar las operaciones militares en el espacio cibernético junto con las operaciones convencionales, un comandante operacional puede aumentar los efectos sobre un enemigo. Cuando Rusia invadió Georgia en agosto de 2008, un ataque de computadoras en red contra los sitios web del gobierno ocurrió simultáneamente junto con la operación convencional. Los ataques a la red inmovilizaron los sitios web del gobierno de Georgia impidiendo las comunicaciones entre los ciudadanos georgianos y, más importante aún, con la comunidad internacional que desconocía la realidad de lo que estaba ocurriendo. Luego de una demora, Georgia usó servidores ubicados fuera del país y cambió los formatos de algunos de sus sitios web para poder continuar con su uso. Al combinar un ataque a una red de computadoras con un ataque convencional, los rusos ampliaron efectivamente los principios de ofensiva, concentración y sorpresa a través de los otros dominios para interrumpir el flujo de la información en Georgia. Los ata-

398 Parks, Raymond C. and Duggan, David P.; Op. Cit.

ques de computadoras en red también actuaron como un apoyo de los fuegos operacionales, dando la forma al campo de batalla al aislar a Georgia internacionalmente. Cuando se usa apropiadamente, el espacio cibernético permite que el comandante operacional aplique los principios de la guerra y los fuegos operacionales agravando sus efectos sobre el enemigo.

Sin embargo, para Parks y Duggan[399], el principio de concentración solo es relevante cuando se ejecutan ataques de denegación de servicio (DOS) que simulan acciones de guerra cinética. Lo mismo ocurre con el principio cinético de la unidad de mando, que solo sería de aplicación a la guerra cibernética en determinadas circunstancias, pues determinados ataques de guerra cibernética utilizan a masas de espectadores que no son conscientes que están siendo usados.

Dado lo relativamente reciente de su empleo masivo es que aún no existe una estructura organizada o un modelo estandarizado para llevar a cabo las operaciones cibernéticas en los niveles estratégico, operacional y táctico y, por esa misma razón, muchas veces la unidad mando o de esfuerzo resulta difícil de aplicar en la guerra cibernética.

Desde su creación en 2009, el U.S. Cyber Command (USCYBERCOM), ha dedicado sus esfuerzos para llevar a cabo misiones de combate en representación de los "comandantes combatientes" (*combatant commanders)*. Ahora éstos, desean emplear las capacidades cibernéticas para impedir la capacidad de un adversario de dirigir sus fuerzas militares, interrumpir o corromper su conocimiento de la situación, asegurar la sorpresa enmascarando la maniobra de las fuerzas propias, tomar el control de plataformas del adversario (vehículos aéreos no tripulados, satélites, etc.) o de procesos logísticos, degradar su infraestructura de apoyo (electricidad, combustible, etc.), crear efectos secundarios que degradan y disminuyen la confianza del adversario en la integridad y confiabilidad de su mando y sus sistemas de control y comunicaciones[400].

La pregunta que surge de esta situación es si es posible integrar los deseos de esos comandantes de teatro cuando el concepto prevaleciente es que las ciberoperaciones son una capacidad nacional y estratégica que debe ser controlada y vigilada de cerca.

Una prueba de que ello resulta difícil de responder es porque inmediatamente surgen otros interrogantes relacionados con el planeamiento de una campaña que deben responderse primero: ¿dónde comienza y termina el espacio cibernético para el Comandante Operacional?, ¿cómo puede diferenciarse una virtual ciberzona de operaciones conjunta de los dominios de tierra, mar y aire definidos por límites geográficos?, ¿en qué difiere la defensa cibernética en un Teatro de Operaciones de lo que se conoce como *Department of Defense information networks*[401] (DoDIN)? ¿Cómo se articula la seguridad

399 Ibídem

400 FitzGerald, Ben F. and Wright, Parker, Lt Col USAF; Digital Theaters: Decentralizing Cyber Command and Control; April 2014; Disruptive Defense Papers; Center for a New American Security; P. 8; Disponible en: http://www.cnas.org/sites/default/files/publications-pdf/CNAS_DigitalTheaters_FitzGeraldWright.pdf.

401 Las operaciones DODIN son acciones tomadas para diseñar, construir, configurar, asegurar, operar, mantener y sostener los sistemas de comunicaciones del Departamento de Defensa de los Estados Unidos y sus redes de una manera que cree y preserve la disponibilidad de datos, integridad, confidencialidad, así como la autenticación de usuario y el no repudio. Ver Joint Publication 3-12 (R); Cyberspace Operations; 5 February 2013; P. vii.

de la información o la seguridad de Internet en el contexto de la defensa cibernética?, ¿cómo diferenciar un ataque cibernético de un incidente de seguridad cibernético?

Una vez que se hayan ordenado, los ataques en la red se mueven a la "velocidad de un rayo" para permitir que las acciones en el espacio cibernético se integren fácilmente con otros dominios. El sostenimiento impone una limitación para un ataque en redes de computadoras. Típicamente, luego de que una víctima identifica un ataque, usualmente repara la vulnerabilidad explotada o elude el sistema, lo que hace que el sostenimiento de ese ataque a esa red de computadoras sea difícil de mantener y, por lo tanto, se dificulte.

Principio de la maniobra

El principio cinético de la maniobra es aplicable a la guerra cibernética. El atacante no mueve sus fuerzas, sólo el punto de ataque. El propósito del principio de maniobra es "colocar al oponente en una posición de desventaja por medio de la aplicación flexible del poder de combate".

Para Scott D. Applegate[402]:

> La cibermaniobra es la aplicación de la fuerza para capturar, interrumpir, negar, degradar, destruir o manipular sistemas de cómputos y recursos de información con el fin de lograr una posición ventajosa respecto a sus competidores. La maniobra en los dominios tradicionales implica principalmente el movimiento de las fuerzas militares y la aplicación de los fuegos operacionales; sin embargo, en el espacio cibernético, obviamente no existe tal movimiento de fuerzas en el sentido cinético ya que es un entorno virtual. Por el contrario, la maniobra en el espacio cibernético implica la aplicación de la fuerza en puntos específicos de ataque o defensa. Esta fuerza es un código escrito especialmente con el propósito de lograr los objetivos del atacante o del defensor y se pone en ejecución en el tiempo y la ubicación virtual de su elección. En un sentido muy real, las fuerzas no se mueven en el espacio cibernético, los que se desplazan son puntos de ataque. Esto es lo que dificulta la detección y observación, muy especialmente en relación con el origen de los ataques.

La cibermaniobra se utiliza para influir en el comportamiento humano y en los de los equipos. Aprovecha su posición en el espacio cibernético para interrumpir, denegar degradar, destruir o manipular recursos informáticos y de información. Se utiliza para aplicar la fuerza, negar operaciones u obtener acceso a fuentes de información clave o sistemas estratégicamente valiosos.

La maniobra lógica en el ciberespacio es, a menudo, una función de los protocolos de seguridad utilizados por sistemas *"host"*[403]. Los sistemas que buscan conectividad con

---

402 Applegate, Scott D.; "The Principle of Maneuver in Cyber Operations"; 2012 4th International Conference on Cyber Conflict C. Czosseck, R. Ottis, K. Ziolkowski (Eds.) 2012 © NATO CCD COE Publications, Tallinn.

403 El término host o anfitrión se usa en informática para referirse a las computadoras conectadas a una red que proveen y utilizan servicios de ella. Los usuarios deben utilizar anfitriones para tener acceso a la red. En general, los anfitriones son computadores monousuario o multiusuario que ofrecen servicios de transferencia de archivos, conexión remota, servidores de base de datos, servidores web, etc.

un "*host*" seguro tendrán más dificultades para acceder que los sistemas que buscan conectividad con aquellos que son inseguros. La defensa contra el ingreso indeseado reside en el código o en la lógica del sistema. Una vez que se establece una conexión entre los sistemas, un potencial intruso debe explotar una falla en la lógica para entrar en el sistema. Un código escrito puede ser una forma de maniobra lógica en el ciberespacio. El potencial intruso escribe un código malicioso para ganar maniobrabilidad frente a sistemas específicos. Cuando un defensor llega a ser consciente de una presencia no deseada dentro del sistema, el defensor modificará el código del sistema para negar la entrada. El intruso que desee permanecer "en el blanco", adaptará el código malicioso en consecuencia. Este proceso es el equivalente al de las fuerzas maniobrando para obtener posiciones ventajosas en los tradicionales dominios del aire, tierra, espacio y mar.

El principio de maniobra, cuando se aplica en el espacio cibernético tiene ciertas características: las acciones pueden ser casi instantáneas y depender solo de la velocidad de las computadoras, pero las reacciones tienden a suceder a una velocidad más lenta dado que requieren de cierta clase de análisis y el compromiso de quienes deben tomar las decisiones; tiene un alcance operacional ilimitado; permite a un atacante mover el punto de ataque hacia adelante y emplear sistemas que son difíciles de atribuir al estado que inicia el conflicto, potenciando de esa manera sus factores de fuerza; la tecnología sobre la cual se basa está en constante evolución, lo cual lleva a cambios constantes en tácticas, técnicas y procedimientos utilizados por los atacantes y defensores en el espacio cibernético. Los métodos que funcionan en la actualidad, pueden no hacerlo en el futuro debido a nuevos e imprevistos avances tecnológicos; a diferencia de los conflictos cinéticos, el terreno del campo de batalla puede modificarse, lo cual permite muy poco espacio para la planificación ya que los ataques son difíciles de atribuir.

Durante varios años el llamado Cyber califato ha sido el arma online esgrimida por el Estado Islámico (EI o ISIS, indistintamente) contra sus enemigos. Su ofensiva incluyó el uso agresivo de los medios sociales y fue noticia de primera plana, anunciando un nuevo frente de la yihad en todo el mundo.

Prometiendo ayuda a ISIS, el Cyber califato hackeó y borró sitios web del gobierno de Estados Unidos, entre los que se incluían los del Comando Central y la sede en Medio Oriente del Pentágono. También atacó objetivos en diversos países, así como, presuntamente, los correos electrónicos secretos de altos funcionarios británicos. El más público de sus ataques fue el de abril de 2015 al canal TV5Monde, donde hackeó su sitio web con el lema *"Je suis ISIS."* Este ataque, visto por millones de personas en todo el mundo, dio al grupo la fama que tanto necesitaba.

En agosto de 2015, un misil lanzado desde un drone hizo impacto en un reducto de ISIS en Raqqa, Siria, y mató a Junaid Hussain, un yihadista británico de 21 años de origen paquistaní que era el hacker más conocido del grupo.

Sin embargo, la inteligencia francesa examinó de cerca al grupo después del ataque de TV5 Monde y concluyó que los hackers involucrados en realidad nada tenían que ver con el Estado Islámico. Más bien, estaban asociados a un hacking colectivo conocido por ser allegados al Kremlin, en concreto APT28, un grupo notorio que es un arma secreta de Moscú, según los expertos de seguridad occidental. En otras palabras, para

Francia, el Cyber califato es una operación de inteligencia rusa ejecutada a través de lo que los espías denominan *cut – out*[404].

Para John Schindler[405], autor de la nota que describe los hechos, el Cyber califato es una operación rusa de las denominadas de falsa bandera, en las cuales los servicios de inteligencia se disfrazan de terroristas para cumplir con sus objetivos. Según el autor, los servicios de inteligencia alemanes y la Agencia Nacional de Seguridad de los Estados Unidos, también arribaron a la misma conclusión que sus colegas franceses.

Principios de simplicidad y seguridad

Para Parks y Duggan, los principios de simplicidad y de seguridad de la guerra cinética son de aplicación en la guerra cibernética. A este último lo denomina "ir tras clientes de menor consumo[406]".

Para Liles y otros[407],

Sin seguridad podría decirse que no existe el vector de ataque de la tecnología de la información y de las computadoras. Lamentablemente, aun los sistemas informáticos más perfectos siguen siendo perfectamente explotables por personas que los utilizan para los propósitos para los que fueran diseñados, pero con resultados nefastos. La literatura describe en detalle las ideas de fallas en cascada y las críticas de la lógica defectuosa. Lo que no se describe son las acciones internas perpetradas por entidades militares como espías y agentes. Esto debería merecer una discusión de carácter clasificado o el hilo conductor de futuras investigaciones.

Mientras que las operaciones de información y operaciones del espacio cibernético pueden emplear las redes de computadoras para alcanzar sus objetivos, son los objetivos mismos los que definen cuál de las dos operaciones se llevan a cabo. El enfoque de las operaciones de información es afectar a las personas del adversario que toman decisiones, al mismo tiempo que protege a las propias. En cambio, el foco principal de las

---

404 En la terminología del espionaje, un cut-out es un intermediario de confianza mutua, un método o canal de comunicación, que facilita el intercambio de información entre agentes. Generalmente sólo saben el origen y el destino de la información a transmitir, pero desconocen las identidades de otras personas involucradas en el proceso de espionaje. Por lo tanto, si fuese capturado no podría ser utilizado para identificar a los miembros de una célula de espionaje.

405 Schindler, John; "False Flags: The Kremlin's Hidden Cyber Hand"; The Observer Digital Newspaper Disponible en: http://observer.com/2016/06/false-flags-the-kremlins-hidden-cyber-hand/

406 En el original se expresa: "we call it going after lowhanging fruit!" En los Estados Unidos, en el mundo de los negocios, el término low hanging fruit se asocia a menudo con la venta de productos de consumo o servicios. Los profesionales de ventas, especialmente aquellos que recién ingresan, primero tienden a buscar a los clientes más fáciles. Por su parte los más experimentados pueden pasar más tiempo buscando las mayores comisiones por ventas a clientes de mayor consumo, dejando a los low hanging fruit detrás para que luego puedan reclamar. Los padres que buscan seguros de bajo costo para niños en edad escolar, por ejemplo, pueden ser considerados low hanging fruit por las compañías de seguros.

407 Liles, Samuel; Rogers, Marcus; Dietz; Eric J. and Larson, Dean; "Applying Traditional Military Principles to Cyber Warfare"; 2012 4th International Conference on Cyber Conflict; C. Czosseck, R. Ottis, Ziolkowski, K. (Eds.); 2012 © NATO CCD COE Publications, Tallinn; Disponible en: https://ccdcoe.org/sites/default/files/multimedia/pdf/3_2_LilesDietzRogersLarson_ApplyingTraditionalMilitaryPrinciplesToCyberWarfare.pdf.

operaciones cibernéticas es utilizar el espacio cibernético para atacar la infraestructura de las tecnologías de la información enemigas, con la intención de negar la libertad de acción en el espacio cibernético al mismo tiempo que protege la propia libertad de acción. Las operaciones de información buscan afectar la toma de decisiones mientras que las operaciones del espacio cibernético se orientan a afectar la libertad de acción en el espacio cibernético[408].

Los nuevos principios de la guerra para la guerra cibernética

Hasta aquí, se ha podido apreciar cómo algunos analistas militares han intentado aplicar los principios tradicionales de la guerra a la guerra cibernética. Sin embargo, según la visión de Steven Metz[409] "pareciera ser más útil tomar una hoja en blanco de papel y comenzar la discusión y debate sobre lo que debe constituir los principios de la guerra cibernética". Es por tal motivo que propone cinco principios novedosos como una manera de enfrentar algo totalmente nuevo como es la guerra cibernética.

Asumiendo como propia la definición de un ex funcionario estadounidense, Richard Clarke, para quien la guerra cibernética consiste en "acciones de un Estado-nación para penetrar en ordenadores o redes de otra nación a los efectos de dañarlos o interrumpirlos," Lenz propone que el primer principio debe ser **concentrarse en los objetivos psicológicos** por cuanto en la guerra cibernética, estos son más importantes que los objetivos físicos pues, a pesar de que es más difícil saber cuándo se ha alcanzado un objetivo psicológico "lo que se hace es menos importante que cómo las audiencias específicas entienden y responden" lo cual significa, que quienes estén involucrados en la guerra cibernética deben poseer, no solo conocimientos técnicos, sino también comprender la psicología de masas.

El segundo principio de Lenz señala que el ***tempo*** – la presión constante - y **la secuencia** son lo que importa para lograr el máximo efecto psicológico, porque las acciones deben llevarse a cabo no sólo cuando es más fácil, sino cuando se maximice el efecto psicológico.

Partiendo de la premisa de que, para disuadir los ataques cibernéticos de otras naciones, Estados Unidos debe tener la capacidad tecnológica de devolver un ataque tanto cibernéticamente como de otras formas y que, además de tener la voluntad política, deben demostrar la capacidad y la voluntad de hacerlo, y que la mejor disuasión es una que los potenciales enemigos más temen, Lenz enuncia como tercer principio **demostrar la capacidad y la voluntad para tomar represalias** tanto simétrica como asimétricamente. Una respuesta simétrica podría ser lanzar un ataque cibernético y una asimétrica, incrementar el apoyo a los opositores al régimen que gobierna el país adversario.

El cuarto principio implica **adaptarse y adecuarse más rápido que los oponentes** pues como escribiera el politólogo Edward Luttwak "*parte de la "lógica paradójica de la*

---

408 Snoddy, David W.; Lt Col, USAF; A Case for Principles of Cyberspace Operations; Research Gate web page, Disponible en: https://www.researchgate.net/publication/235142916_A_Case_for_Principles_of_Cyberspace_Operations.

409 Metz, Steven; It's Time to Begin Thinking About the Principles of Cyberwar; World Politics Review Web Page, Disponible en: http://www.worldpoliticsreview.com/articles/16354/it-s-time-to-begin-thinking-about-the-principles-of-cyberwar.

estrategia" es que lo que funciona hoy puede no funcionar mañana debido a que los opositores se adaptan y ajustan". Esto sucede también en la guerra cibernética, pero en un ciclo de tiempo mucho más comprimido donde es necesario no sólo idear nuevos métodos de ataque y defensa, sino también desarrollar nuevos conceptos y organizaciones, a menudo mientras que se está empeñado en el conflicto.

Por último, el quinto principio de Lenz, es **identificar los umbrales de autoridad nacional para atribuir un ataque, y los niveles aceptables de daño colateral.** Ello se debe a que, como se ha reiterado varias veces en esta obra, en la guerra cibernética resulta difícil identificar al autor de un ataque y la precisión es difícil de lograr en los ciberataques, a menos que el objetivo esté desconectado del resto de la red de información, algo que no será común que suceda. En muchos casos, los ciberataques pueden tener resultados en cascada, a menudo impredecibles a lo largo de una nación y, aún más importante, en todo el mundo. Por ello, Lenz recomienda a los planificadores saber lo que las autoridades consideran aceptable en términos de estándares de reconocimiento y niveles de daños colaterales, cuando se desarrollan las operaciones propias.

Si bien estos principios enunciados por Lenz son específicamente para Estados Unidos, no dejan de mostrar otra forma de encarar la temática respecto de cuáles serían los principios que debieran aplicarse a la guerra cibernética.

En particular, el quinto principio es un fiel reflejo de lo que en los Estados Unidos se conocen como los Principios de la Acción Militar Conjunta, los cuales, a los tradicionales principios de la guerra que sostiene la doctrina estadounidense agregan los siguientes:

- **Restricción** – para limitar el daño colateral y evitar el uso innecesario de la fuerza. Este principio requiere el equilibrio cuidadoso y ordenado de la necesidad de seguridad, la conducción de operaciones militares y el estado final estratégico nacional.
- **Perseverancia** – para asegurar el compromiso necesario para alcanzar el estado final estratégico nacional. Las causas subyacentes de la crisis pueden ser escurridizas, haciendo que sea difícil de lograr la solución definitiva. La paciente, firme y persistente búsqueda de objetivos y metas nacionales es, a menudo, esencial para el éxito.
- **Legitimidad** – para mantener la autoridad legal y moral en la ejecución de las operaciones. La Legitimidad, que puede ser un factor decisivo en las operaciones, se basa en la legalidad real y percibida, la moralidad y la rectitud de las acciones de las diferentes perspectivas del público interesado.

Parks y Duggan[410] explican claramente las razones por las cuales los principios de la guerra cibernética son diferentes a los de la guerra convencional:

La guerra cibernética es diferente de la guerra convencional, cinética. Tanto ella como la guerra de la información dependen de la fragilidad de los seres humanos por muchas características. Una de las diferencias fundamentales entre la guerra cibernética y

410 Parks, Raymond C. and Duggan, David P. "Principles of Cyber-warfare". Op. Cit.

la guerra cinética es la naturaleza de sus entornos. La primera tiene lugar en el mundo físico, regido por leyes físicas que se conocen y entienden. La segunda tiene lugar en un mundo artificial, hecho por el hombre que es caótico y con imperfecciones. La guerra cibernética puede utilizar algunos de los principios de la guerra cinética, pero hay otros principios que tienen poco o ningún significado en el espacio cibernético. Por estas razones, los principios de la guerra cibernética son, en última instancia, diferentes de los de la guerra cinética.

Las operaciones cibernéticas y el Plan de Campaña

A lo largo del tiempo, la planificación y ejecución de la guerra ha comenzado con un análisis del enemigo. Tradicionalmente, ese estudio incluía el examen de las organizaciones sociales, culturales y políticas del adversario, la manera en que este comerciaba y se relacionaba con otros grupos y quizás, lo más importante, cómo el adversario veía y llevaba a cabo la guerra. En cada caso, estos estudios se realizaban con la finalidad de desarrollar las formas de derrotarlo.

Sin embargo, en la actualidad, la información es cada vez más fundamental para que un planeamiento sea efectivo y la ejecución de operaciones de combate resulten eficaces, razón por la cual, debe extenderse más allá de la simple comprensión del espacio de batalla que ofrecen los diferentes sensores. Quienes deban tomar decisiones, los planificadores y quienes ejecutan las operaciones necesitan tener acceso a mucho más que una lista estándar de posiciones militares, de equipos, de entrenamiento y de tácticas.

Hoy en día, la información e inteligencia sobre los sistemas de comunicación y las redes eléctricas del enemigo, sus medios de transporte y obras públicas de infraestructura y estructura incluso social, instituciones y actores políticos pueden y deben ser, cuando sea posible, recogidos, analizados, difundidos y explotados. En este sentido, no se debe esperar ninguna posibilidad de conflicto, sino transformarse en actividades rutinarias de prevención. Es por tal razón que las funciones de inteligencia y comunicaciones deben integrarse más estrechamente con las operaciones del ciberespacio.

Por otra parte, para Milan Vego[411] las operaciones cibernéticas en el nivel operacional también:

> ...pueden ser representadas como equivalentes a los fuegos operacionales - la aplicación letal o no letal del poder de fuego para generar un impacto decisivo en el trascurso y el resultado de una campaña u operación importante. Hoy en día, representan una función inherentemente conjunta. No son simplemente operaciones de apoyo de fuego; por lo tanto, el éxito de una maniobra operacional no es necesariamente dependiente de estos fuegos. Sin embargo, pueden facilitar la maniobra operacional. Se llevan a cabo en las profundidades operacionales o estratégicas de las defensas del enemigo.

Pero, en definitiva, lo que logra los objetivos de la campaña es la integración de las operaciones en tierra, mar, aire, espacio y espacio ciberespacio.

---

411 Vego, Milan N.; Joint Operational Warfare Theory and Practice. Newport RI: (Naval War College, 2009), VIII-59-60

Las operaciones cibernéticas y el arte y diseño operacional

Al igual que otras capacidades, las operaciones cibernéticas deben ser optimizadas en todas las fases de la campaña comprendiendo cómo estas acciones aprovechan la ventaja del punto decisivo, influyen sobre los centros de gravedad operacionales o estratégicos y cómo apoyan la consecución de los objetivos operacionales.

Para la Publicación PC 20-01[412]:

El arte operacional es la forma creativa en que se combinan los elementos del diseño operacional a través de la estructuración eficiente de acciones tácticas en espacio, tiempo y propósito, con un balance entre riesgo y oportunidad, para crear y mantener condiciones necesarias afines al logro de objetivos del propio nivel o del nivel superior de la conducción. En el Nivel Operacional resultará de suma importancia armonizar la disponibilidad de recursos para alcanzar fines, e implicará el uso creativo de esos recursos para diseñar caminos o métodos para alcanzarlos.

Asimismo, "Los elementos del diseño operacional considerados son: el Estado Final Deseado, el Centro de Gravedad, los Puntos Decisivos, las Líneas de Operaciones, el Momento y el Ritmo"[413, 414].

De una forma más coloquial, podría decirse que el Arte Operacional comienza con dos preguntas básicas: ¿Cuáles son los objetivos de quien comanda las operaciones? ¿Qué efectos está tratando de lograr? La idea de ganar una guerra mediante una única y decisiva batalla es una noción puramente táctica. Es justo la antítesis del arte operacional y del nivel operacional de la guerra, en que las claves son las operaciones sucesivas y los efectos acumulativos, y en esto consiste el arte operacional.

Para Crowell[415] algunos de los desafíos que enfrentan los comandantes operacionales son conocer dónde y cómo se emplean las operaciones en el espacio cibernético. Por ejemplo, cuando una bomba cae sobre un objetivo, ¿provino de un avión tripulado o de un vehículo aéreo no tripulado?; ¿el atacante emplea capacidades cibernéticas para alcanzar el objetivo?; ¿cómo podría el vehículo aéreo no tripulado haber sido interceptado, si se hubiese atacado el espectro electromagnético?; ¿cómo son los vínculos entre el vehículo y el controlador?; ¿dónde se encuentran?; si el adversario ha trastocado el espectro electromagnético, ¿puede seguir usándolo el comandante?; ¿cuáles son los objetivos de la operación del espacio cibernético?; ¿son objetivos físicos o cognitivos?

Por lo tanto, desde el punto de vista de las operaciones cibernéticas de defensa, de explotación y de ataque que constituyen las denominadas operaciones de red de computadoras (*Computer Network Operations*), en el planeamiento se deberían:

---

412 República Argentina. Ministerio de Defensa, Estado Mayor Conjunto, PC 20-01 Planeamiento para la Acción Militar Conjunta Nivel Operacional P. 15.

413 Ibidem; P. 18.

414 Es por ello que, en esta parte de la investigación se hablará del ciber centro de gravedad, de ciber líneas de operaciones, de los ciber puntos decisivos y del ciber estado final deseado.

415 Crowell, Richard M. War in the Information Age. Op. Cit.

a. Determinar los hechos conocidos, el estado actual o las condiciones de las fuerzas conjuntas.
b. En coordinación con el C2 analizar algunos de los siguientes aspectos del adversario:
   1. Determinar la dependencia del adversario sobre el uso del espectro electromagnético.
   2. Determinar la capacidad de ataque cibernético y de comunicaciones del adversario.
   3. Determinar la capacidad de recolección de inteligencia del oponente.
   4. Analizar las vulnerabilidades propias de C2 y C4I relacionadas con el ataque cibernético y de comunicaciones.
c. Desarrollar hipótesis para reemplazar datos faltantes o desconocidos.
d. Analizar la misión del comandante y su intención desde el punto de vista cibernético.
e. Determinar las limitaciones.
   1. Qué debe hacerse (imposiciones).
   2. Qué no puede hacerse (restricciones).
   3. Otras limitaciones (políticas, legales, diplomáticas, etc.).
f. Determinar los centros de gravedad propios y del adversario y los puntos decisivos tentativos.
   1. Determinar los posibles Centros de Gravedad del adversario.
   2. Determinar las formas de ayudar en la protección de los Centros de Gravedad propios.
g. Identificar las tareas a llevar a cabo.
   1. Determinar las tareas explícitas.
   2. Determinar las tareas implícitas.
   3. Determinar las tareas de los subordinados.
   4. En función de las tres anteriores determinar las tareas y objetivos de las operaciones cibernéticas.
h. Analizar la estructura de las fuerzas propias a fin de establecer la disponibilidad adecuada de medios para llevar a cabos las tareas.
i. Efectuar un análisis de riesgos.
j. Determinar el estado final desde el punto de vista cibernético.

El análisis de la situación cibernética

El conocimiento y la comprensión de la situación requieren de una oportuna y precisa evaluación de las operaciones propias y del enemigo dentro del espacio de batalla, con el fin de facilitar la toma de decisiones.

En el espacio cibernético, el área de interés que debe analizarse no está limitada por fronteras nacionales o naturales. Por ello, normalmente incluye ciber-personas, estructuras y actividades sobre las que el comandante es capaz de influir o que están bajo el control del adversario y podrían llegar a obstaculizar o impedir el cumplimiento de la misión. El área de interés es global por naturaleza, pero para limitar su alcance se pueden evaluar ciertos factores que podrían ser clave en el espacio cibernético.

En las doctrinas militares, cualquier localidad o área, cuya ocupación o retención brinda una marcada ventaja a un atacante o a un defensor es considerada como un factor relevante, pues puede llegar a influir o ser utilizado para el cumplimiento de la misión. Cuando se aplica al terreno geográfico, esta definición es clara, pero en el espacio cibernético, si bien pueden existir ciertas similitudes, también puede haber diferencias significativas. Algunos consideran que en el espacio cibernético esos factores están representados por *routers, switches,* cables y otros dispositivos que se encuentran en todos los planos del espacio cibernético, los cuales incluyen las dimensiones geográficas, físicas, lógicas, de las personas y de supervisión[416] y que muchas veces no están ligados a una ubicación específica, o la ubicación geográfica puede ser irrelevante.

En el nivel operacional, esos factores pueden incluir servidores de comando y control que se utilizan para supervisar ataques informáticos a gran escala basados en *botnets*. Una cuenta del administrador del sistema puede considerarse un factor clave si la posesión de esa cuenta pudiera ser utilizada por un atacante para comprometer recursos del defensor, como podría ser el sistema de nombres de dominio (en inglés *Domain Name System* o DNS)[417].

Para Raymond y otros[418],

> ...los ataques recientes por hackers del Ejército Electrónico Sirio (SEA) contra el New York Times y otras organizaciones destacan las vulnerabilidades potenciales inherentes en no reconocer un factor clave del ambiente cibernético en el plano lógico; el SEA alcanzó su objetivo de desfasar el sitio web del New York Times atacando el registrador de nombres de dominio[419] en lugar de dirigirse directamente a los sitios web propiamente dichos, que podrían haber estado mejor defendidos.

En el plano físico, un factor clave podría ser un dispositivo inalámbrico mal configurado que utilice un protocolo de seguridad obsoleto, y una ubicación geográfica podría ser la ubicación de la infraestructura de apoyo a las operaciones cibernéticas, tales como centrales eléctricas y los controles de los sistemas de ventilación, calefacción y aire acondicionado (HVAC).

Según el punto de vista de Raymond,

---

416 Raymond, David; Cross, Tom; Conti, Gregory and Nowatkowski, Michael; Key Terrain in Cyberspace: Seeking the High Ground; 2014 6th International Conference on Cyber Conflict; 2014; Disponible en https://ccdcoe.org/sites/default/files/multimedia/pdf/d2r1s8_raymondcross.pdf

417 Utiliza una base de datos distribuida y jerárquica que almacena información asociada a nombres de dominio en redes como Internet. Aunque como base de datos el DNS es capaz de asociar diferentes tipos de información a cada nombre, los usos más comunes son la asignación de nombres de dominio a direcciones IP y la localización de los servidores de correo electrónico de cada dominio.

418 Ibídem.

419 Un registrador de dominios es una empresa que vende dominios de Internet y que permite que un individuo o empresa pueda pagar una cuota anual a cambio de tener un nombre de dominio, como .com, .co, .es, .org, .net, y muchos otros

> ...quien se defiende, debe comenzar su análisis de la situación mediante la identificación de los sistemas de información o datos que pueden ser pasibles de ser atacados. Es importante tener en cuenta que los activos que son más valiosos para una organización no siempre son los activos más valiosos para los atacantes. Aunque organizaciones prudentes consideran siempre los riesgos para sus "joyas de la corona", los atacantes pueden ser interesados en otros activos, así como la palabra clave de inicio de sesión de un auxiliar administrativo.

Por lo tanto, en el análisis de la situación será necesario preguntarse, entre otras cosas: ¿cuáles son (todos) los diferentes vectores que pueden utilizarse para acceder a cada sistema pasible de ser atacado? Es importante considerar todas las interfaces que el sistema tiene con el mundo exterior y que el atacante podría aprovechar en cada plano del espacio cibernético, ya sean interfaces de redes directas o indirectas como medios extraíbles o claves personales de acceso físico.

¿Desde qué ubicaciones el atacante puede acceder a cada sistema pasible de ser atacado? En este punto, el análisis puede ser iterativo si el atacante puede llegar a una interfaz del sistema a través de una red o sistema en particular. Es importante enumerar las avenidas de aproximación a ese sistema secundario o red y determinar la ubicación desde la cual esas avenidas de aproximación pueden ser alcanzadas y así sucesivamente.

¿Hay particulares puntos de vista que le dan a un oponente la oportunidad de atacar determinados sistemas? En la mayoría de las redes existen componentes de infraestructura que podrían proporcionar un amplio acceso del atacante a muchos sistemas en la red, como sistemas de gestión de identidad y acceso, cortafuegos, copias de seguridad y sistemas de gestión de punto final.

En síntesis, quienes analicen la situación cibernética deberían, al menos, formularse los siguientes interrogantes: ¿cuáles son las amenazas/riesgos para la propia red?; ¿hay indicios de que un ataque vaya a ser concretado o se está ejecutando?; ¿por parte de quién?; ¿qué es lo crítico dentro de la propia red para el desarrollo de la operación?; la red, ¿es confidencial e integral o es vulnerable a un ataque?; ¿qué se conoce sobre la ubicación y las capacidades del enemigo en el ambiente cibernético?

Todas estas preguntas tendrán diferente respuesta según sea la capacidad cibernética del adversario. Un país pobremente desarrollado donde los controles cibernéticos no operados por la inteligencia humana sean mínimos, no tendrá mucha vulnerabilidad en este campo para ser atacado. No obstante, podrán encontrarse instalaciones peligrosas como represas o centrales nucleares con sistemas operativos viejos cuyos fabricantes ya han desistido del apoyo de seguridad. Estas fallas de seguridad inaceptables deben ser conocidas como trabajo previo porque las posibilidades de accidentes de magnitud son posibles, sin que exista siquiera posibilidad de conflicto armado. Estas actividades cibernéticas son del nivel operacional porque van a afectar la maniobra y la logística de las tropas que participen.

Para Raymond, en el nivel operacional estos factores relevantes se caracterizan por dar a un adversario una ventaja durante la campaña y señala que

> ...un componente clave de Stuxnet, involucró, por ejemplo, archivos de controlador de software firmados por certificados digitales legítimos de dos empresas que aparentemente fueron comprometidas como parte del desarrollo de ese malware. Los sistemas informáticos que esas empresas utilizaron para almacenar sus certificados digitales constituyeron un factor clave. Los creadores de Stuxnet fueron capaces de obtener, de esas computadoras, un medio que les proporcionaron una ventaja cuando fueron tras su objetivo primario.

Todo esto puede considerarse como factores clave para el análisis de la situación en el espacio cibernético. Una vez identificados estos factores, se podrán comenzar a tomar medidas para proteger aquellos sistemas pasibles de ser atacados.

Seguramente, se requerirá de un conocimiento técnico mucho más profundo de la situación cibernética por parte de personas más calificadas para poder identificar y aprovechar los factores clave en el espacio cibernético, pero el desarrollo de estas ideas podría ser de utilidad para concentrar los limitados medios cibernéticos en el camino más probable hacia el éxito durante las operaciones ofensivas o defensivas. Una de las vulnerabilidades que tienen los países en desarrollo es que existe una marcada diferencia entre estrategas cibernéticos y técnicos cibernéticos, los expertos son realmente escasos y las disputas se centran en la adquisición de equipos extranjeros, cuyos algoritmos son conocidos únicamente por los fabricantes. Sería algo equivalente a comprarle radios a los británicos o a alguno de sus aliados para intentar recuperar las Malvinas.

En cuanto a las limitaciones[420], es sabido que en la Directiva de Planeamiento podrán aparecer ciertos condicionamientos que le son impuestos al comandante y que de una manera u otra lo limitan, como por ejemplo las dimensiones del Teatro de Operaciones, los medios humanos y materiales que le asignan, el tiempo que le exigen para cumplir con la misión, los métodos para emplear el poder de combate y las listas de los objetivos que no pueden ser batidos, (*No - Strike Lists*), entre otros.

En el espacio cibernético, la naturaleza del dominio fue hecha por el ser humano y, por lo tanto, su estructura puede ser cambiada para ajustarlo mejor a las demandas operacionales y al cumplimiento de la misión. Es donde un Comandante Conjunto llevará a cabo las operaciones para cumplir una misión. No obstante, para crear un área cibernética conjunta, se necesita un estratega cibernético que no se forma en un año. Otro requerimiento podría ser habilitar las medidas equivalentes al control operacional en el Área de Operaciones Cibernéticas conjuntas.

Se dificulta un poco la comprensión porque suele pensarse que para delinear un área se requiere de un mapa donde se puedan trazar líneas. En el espacio cibernético, que es virtual, estas líneas se logran cuando se aplican tecnologías existentes que permitan implementar medidas de control. Estas medidas de control cibernético son paralelas y

---

420 Limitación: en el contexto del Planeamiento para la Acción Militar Conjunta condicionamientos que le son impuestos al Comandante por la Autoridad Superior y que de una manera u otra limitan su libertad de acción. Refieren, sin que la enumeración sea exhaustiva, a las dimensiones del Teatro de Operaciones, los medios humanos y materiales que se le asignan, al tiempo exigido para cumplir con la misión, los métodos para emplear el poder de combate. PC 20-01, 2017

similares a las empleadas en los dominios territoriales, tales como autoridades escalonadas, relaciones de comando definidas y flexibilidad en las operaciones estratégicas, operacionales y tácticas.

Así, se define como Área de Operaciones Cibernéticas Conjuntas a los sistemas de los medios cibernéticos amigos y propios que el Comandante de Fuerzas Conjuntas requiere para poder ejercer eficientemente el Comando y Control de sus fuerzas. Es importante distinguir que el Área de Operaciones Cibernéticas Conjuntas no necesariamente refleja con exactitud el Área de Operaciones Conjuntas geográficas.

Parte de los sistemas de Comando y Control suelen encontrarse físicamente en el espacio geográfico del Área de Operaciones, pero puede ocurrir que partes significativas de la arquitectura no lo estén. Esta es otra distinción importante en las áreas geográficas y las áreas virtuales. Al respecto, también afecta la consideración del Área de Interés cibernética, mucho más amplia que el Área de Interés geográfica, ya que un enemigo cibernético puede atacar desde cualquier lugar del mundo. Por lo tanto, el espacio cibernético enemigo puede ser mejor definido desde el punto de vista de Área de Interés que desde el de Área de Responsabilidad. Luego, los efectos que pueda requerir un Comandante Conjunto con influencia en su misión operacional se van a encontrar fuera de su jurisdicción geográfica y deberán establecerse políticas de intrusión al respecto para evitar asociar el concepto de área geográfico al concepto de área cibernética.

En lo que respecta a las imposiciones[421] (qué debe hacerse) y restricciones[422] (qué no puede hacerse) para Williams Brett[423] las principales imposiciones vendrán de parte de la política, de las reglas de empeñamiento y de la autorización para ejecutar las operaciones cibernéticas. *"Estamos siendo desafiados por el hecho de que estas imposiciones están en constante evolución tanto como ocurre con el ambiente cibernético y la comprensión del cambio del ambiente"*.

> El segundo conjunto de límites describe las mismas restricciones asociadas con cualquier blanco. El planificador debe contar con el apoyo de inteligencia para entender cómo funciona el blanco, cómo se accede al mismo y la capacidad de impactarlo para generar el efecto deseado. La selección de blancos en el espacio cibernético es complicada por la naturaleza cambiante de los sistemas de los blancos, el desarrollo de extenso destino requerido para alcanzar una solución y nuestra capacidad incipiente para describir efectos deseables e indeseables para las operaciones del espacio cibernético[424].

En lo que respecta a las imposiciones legales, precisamente como el Derecho Internacional de los Conflictos Armados no establece la forma en que debe aplicarse a las

421 Imposición: en el contexto del Planeamiento para la Acción Militar Conjunta es una orden dada a un comandante por una Autoridad Superior que impone la ejecución de una acción y que por lo tanto restringe su libertad de acción. PC 20-01, 2017

422 Restricción: en el contexto del Planeamiento para la Acción Militar Conjunta es una orden dada a un comandante por una Autoridad Superior que prohíbe la ejecución de una acción y que por lo tanto restringe su libertad de acción. PC 20-01, 2017

423 Williams, Brett T.; The Joint Force Commander's Guide to Cyberspace Operations; Joint Force Quarterly 73; April 01, 2014; P. 32.

424 Ibídem.

operaciones cibernéticas y es probable que continúen las discusiones, son los propios Estados quienes determinan sus puntos de vista en respuesta a los incidentes cibernéticos. No obstante, debe recordarse que los principios de necesidad, proporcionalidad e inminencia siempre serán de aplicación.

También debe tenerse presente que no todas pueden ser consideradas ciberoperaciones. Para el *Law of War Manual*[425] las operaciones dirigidas contra las capacidades cibernéticas de un adversario, pero que no se consiguen en o a través del espacio cibernético, no se consideran operaciones cibernéticas. Por ejemplo, el bombardeo de un concentrador de red (*hub*)[426], o la interferencia de las comunicaciones inalámbricas, no sería considerada como tal, aunque su destrucción permita lograr objetivos militares en el espacio cibernético.

> Ciertas operaciones cibernéticas pueden tener un paralelo claro con las operaciones cinéticas en términos de sus capacidades y los efectos que crean. Existen casos bien definidos donde los efectos físicos de una acción cibernética ofensiva serían comparables a lo que podría lograr una acción cinética: por ejemplo, la destrucción por medio de una bomba de una represa y la inundación de una población civil podría también lograrse fácilmente mediante la inserción de un código malicioso desde una computadora lejana. Sin embargo, hay otros tipos de acciones cibernéticas que no tienen un paralelo claro cinético y que plantean serias cuestiones sobre exactamente qué significa el uso de la fuerza. Este tipo de operaciones puede tener implicancias muy diferentes a las presentadas por ataques con armas tradicionales, y esas implicancias bien pueden producir conclusiones diferentes[427].

El ambiente cibernético, al igual que los otros cuatro dominios físicos, tiene características distintivas que requieren una doctrina especializada, una política de empleo, recursos estandarizados entre las Fuerzas Armadas y expertos en el tema. Debido a su reciente aparición, el espacio cibernético es más dificultoso de comprender porque no es fácil adentrarse en un espacio virtual, pero si se habla del nivel operacional de guerra, se encuentra que tiene muchísimas similitudes con los otros dominios. En lo único que hay que cuidarse es en las analogías erróneas que por simplistas pueden llevar a error. El primer impulso al comparar dominios es equiparar al espacio con el cibernético, ya que tienen la característica común de no tener fronteras. Sin embargo, esta analogía es simplista, porque existen soluciones técnicas que permiten atenuar las limitaciones que surgen de la falta de límites geográficos en el espacio cibernético.

Sin embargo, hay otras características que permiten asociar más al espacio cibernético con los tres dominios territoriales. Por ejemplo, en el espacio cibernético pueden apreciarse efectos tanto en el nivel estratégico, como en el operacional y en el táctico, lo que no ocurre en el dominio espacio. También, en el espacio cibernético convergen

---

425 US Department of Defense; Law of War Manual; 2015; P. 994.

426 Concentrador (hub) es el dispositivo que permite centralizar el cableado de una red de computadoras, para luego poder ampliarla.

427 US Department of Defense; Law of Force Manual; 2105, P. 998.

actores civiles internos e internacionales, comerciales y gubernamentales, los que van a influenciar a las operaciones cibernéticas del Ministerio de Defensa. Luego, tal como ocurre con los dominios territoriales, habrá que preocuparse del fratricidio, de los no combatientes, de los daños colaterales, de la proporcionalidad, de la discriminación y de las reglas de enfrentamiento. Otra similitud más del dominio cibernético es que al igual que los dominios territoriales, los combatientes pueden introducir nuevas capacidades, métodos, técnicas y procedimientos mucho más rápido que en el espacio, y en el espacio cibernético ello ocurre de manera más rápida que en cualquier otro dominio.

El centro de gravedad cibernético

La palabra *Schwerpunkt* definida en el diccionario como centro de gravedad, etimológicamente significa "punto pesado". Es donde debe colocarse todo el esfuerzo si se aspira a obtener el éxito, sin distraerse en objetivos secundarios. Es lo que Clausewitz llamaba "principio de masa", y Foch "principio de economía de fuerzas". En el nivel operacional de guerra, el esfuerzo principal cibernético está en la defensa. Curiosamente, la mayoría de la bibliografía se refiere a los ataques cibernéticos, y a los ataques a redes de computadoras y eso probablemente sea porque las operaciones ofensivas cibernéticas requieren de mayor marco legal y mayores consideraciones operacionales. No obstante, lo que garantiza un correcto funcionamiento del propio comando y comunicaciones es la habilidad para defender los sistemas y las redes de computadoras. Es por ello que, en el espacio cibernético, la seguridad cibernética es inicial, para luego, en caso de ser necesario, dar lugar a la defensa.

Esta es una de las características distintivas del espacio cibernético, ya que en los otros dominios la forma de ganar y mantener la superioridad es mediante la ofensiva. En este sentido, el dominio cibernético cumple con el axioma de Clausewitz de la superioridad de la defensa sobre el ataque. Por ahora, hasta que se simplifique identificar la atribución, se normalice la ley internacional, y se consoliden las propias capacidades, ellas serán limitaciones para obtener superioridad en el espacio cibernético, y habrá que confiar en una arquitectura de Comando y Control robusta, que pueda ser defendida, flexible y variada, que pueda absorber el asalto enemigo y aún en esas condiciones, estar lista para proporcionarle un comando y control seguro al Comandante Conjunto en el cumplimiento de su misión operacional.

En lo que hay que ser cuidadosos es en que, en el ambiente cibernético, el concepto de punto culminante tiene un efecto inverso al de los dominios territoriales. En las operaciones convencionales, el punto culminante se alcanza cuando se agota la ofensiva, pero en el dominio cibernético, a la inversa, si un ataque progresa, el ataque se robustece porque el *malware* se expande sin control. A pesar de esto y hasta que el conocimiento técnico progrese, la defensa del comando y control propio que asegure el ejercicio de una defensa dinámica y flexible será el requisito del éxito para continuar operando.

El comandante y su Estado Mayor realizan el análisis del o de los Centros de Gravedad durante la planificación militar con la finalidad de identificar las capacidades críticas, los requerimientos críticos y las vulnerabilidades críticas tanto propias como del enemigo.

Dado que cada vez es mayor la ciberdependencia, ello se traduce en una vulnerabilidad crítica, razón por la cual los comandantes operacionales deben centrar sus esfuerzos en la defensa cibernética para proteger las redes esenciales y permitir el empleo eficaz de sus sistemas de armas dependientes de la cibernética.

Para Karaman, Catalkaya, Gerehan y Goztepe[428]

En el análisis del centro de gravedad, hay varias preguntas que deben ser respondidas: ¿cuál es el estado final que desea el enemigo?, ¿qué tipo de actividades puede realizar el enemigo para alcanzar el estado final?, ¿qué requerimientos apoyan tal actividad del enemigo?, ¿qué actividades impiden alcanzar el propio estado final? En el análisis del centro de gravedad, se puede obtener la ventaja del análisis de los factores cibernéticos que consisten en las capacidades críticas propias y del enemigo, las misiones y las vulnerabilidades.

Para Héctor Gómez Arriagada[429],

Las ciberoperaciones no son una cuestión técnica, ni administrativa, ni logística; son un asunto de operaciones. Las defensivas dan protección a sistemas y procedimientos vitales para las operaciones propias, mientras que las ofensivas contribuyen concretamente a degradar las capacidades enemigas. En ambos casos, actúan sobre potenciales centros de gravedad.

Para E. Lincoln Bonner III[430],

> Los Centros de Fusión de Datos son centros de gravedad en el espacio cibernético porque es por donde pasa la orientación. Los Centros de Fusión en el nivel operacional incluyen los nodos de mando y control y los nodos de procesamiento, explotación y difusión de la información de inteligencia, vigilancia y reconocimiento del enemigo. Destruyendo, degradando o neutralizando estos Centros de Fusión de Datos, se limitará la efectividad operacional del adversario para orientar y concentrar los efectos en tiempo y/o espacio. Independientemente del camuflaje, ocultamiento y capacidad de engaño del enemigo para evitar ataques cinéticos, los Centros de Fusión de Datos deben, hasta cierto punto, anunciar su ubicación en el espacio cibernético (por ejemplo, dirección IP) para poder recibir datos y distribuir información. Casi siempre suelen ser vulnerables a ataques cibernéticos ya que su utilidad depende largamente de

428 Karaman, Muhammer; Catalkaya, Hayrettin, Gerehan, Ahmet Zeki and Goztep, Kerim e; Cyber Operation Planning and Operational Design; Operations and Intelligence Turkish Army War College; Disponible en: http://r.search.yahoo.com/_ylt=AwrBTvjBaOdXpEcAYnSr9Qt.;_ylu=X3oDMTBydWNmY2MwBGNvbG8DYmYxBHBvcwM0BHZ0aWQDBHNlYwNzcg--/RV=2/RE=1464327234/RO=10/RU=http%3a%2f%2fsdiwc.net%2fdigital-library%2fweb-admin%2fupload-pdf%2f00001773.pdf/RK=0/RS=_VFyxtxDIW_.LiLIDWfE9VH6kSY-.

429 Gómez Arriagada, Héctor Us Cyber Command, Op. Cit.

430 Bonner, E. Lincoln III; Cyber Power in 21st -Century Joint Warfare; Joint Force Quarterly 74, 3rd; Quarter 2014; P. 108.

su conectividad porque el poder de una red crece exponencialmente con el número de usuarios. Si los nodos no están ampliamente conectados, son irrelevantes al esfuerzo bélico del enemigo y, por lo tanto, pueden ser ignorados.

Para la doctrina del Ejército Popular de Liberación chino, *"La logística de los Estados Unidos y los sistemas C4ISR son los más importantes centros de gravedad para apuntar en un conflicto"*[431]. Según Krekel y otros[432]:

...los analistas chinos sugieren que "los comandantes chinos seguramente intentarán atacar estos sistemas con contramedidas electrónicas y equipos de ataque y explotación de red, probablemente antes de un combate real a fin de retrasar el ingreso de los Estados Unidos en un conflicto, o degradar sus capacidades.

Un Comandante Conjunto debe tener en cuenta no solo la arquitectura cibernética militar del enemigo dentro de su área de operaciones, sino tener una visión de los elementos no militares con capacidad de operar contra sus sistemas cibernéticos de comando y control desde su área de interés. No obstante, las interacciones son complejas, las autoridades y responsabilidades se superponen, algunas autoridades propias cibernéticas pueden erróneamente pretender micro-controlar las actividades del Comandante Conjunto en este ámbito, porque aún no se ha desarrollado la absoluta comprensión del ambiente cibernético.

Para asegurarse la comprensión del ambiente cibernético, es necesario cerciorarse que en el análisis del Centro de Gravedad se incluya al espacio cibernético. Eso va a permitir identificar capacidades críticas, requerimientos y vulnerabilidades cibernéticas y ayudar al Comandante a identificar avenidas de aproximación importantes y terrenos clave cibernéticos para concentrarse en el esfuerzo defensivo. Igualmente, se debe ser consciente de que habrá que identificar lo importante para concentrar los esfuerzos defensivos en ese lugar, ya que materialmente no es posible defender todo con la misma dedicación.

Las capacidades, vulnerabilidades y requerimientos críticos en las ciberoperaciones

Para ejercer el Comando y Control, un Comandante Conjunto debe conocer la arquitectura del sistema, la cual, para Williams[433], puede ser concebida como si tuviese cinco componentes: sensores que entregan inteligencia, vigilancia y reconocimiento; una

431 Wortzel Larry M.; The Chinese People's Liberation Army and Information Warfare; Op. Cit. U.S. Army War College, Strategic Studies Institute; Marzo 2014; Disponible en: http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA596797

432 Krekel, Bryan; Adams, Patton and Bakos, George; Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage; The Washington Post, March 7, 2012; P. 9; Disponible en: https://www.washingtonpost.com/r/2010-2019/WashingtonPost/2012/03/08/National-Security/Graphics/USCC_Report_Chinese_Capabilities_for_Computer_Network_Operations_and_Cyber_%20Espionage.pdf.

433 Williams, Brett, T. Ten propositions regarding cyberspace operations; Joint Force Quarterly 61; 2° quarter 2011; P. 13

infraestructura de comunicaciones que incluye redes alámbricas e inalámbricas; redes que organizan y distribuyen información; capas de protección que requieren identificación, autorización, control de acceso y seguridad física y virtual; y *conocimiento de herramientas para la decisión y ayuda para el proceso de toma de decisiones* para desplegar la información de manera tal que facilite la toma de decisiones.

Para la PC 20-01[434],

> Una debilidad representará un elemento vital dentro de la situación o del sistema propio o enemigo y que, al poder ser explotado con los medios de que se dispone, se constituirá en una vulnerabilidad. Una vulnerabilidad constituirá el foco hacia donde se materializarán las acciones dentro de cada Modo de Acción (MA), con el objeto de degradar, afectar o neutralizar al enemigo o sus Centros de Gravedad (CDG).

Para Williams Brett[435]

> ...en el análisis de la situación se puede determinar rápidamente cuándo existen muchos sistemas involucrados, todos con sus propias vulnerabilidades, a las que se suman vulnerabilidades adicionales en los puntos donde se conecta un sistema con otro. Esas serían las vulnerabilidades que se podrían abordar y, por lo tanto, priorizar los esfuerzos para contrarrestar la capacidad específica del adversario que intente interferir en nuestro terreno cibernético clave. Vinculando las vulnerabilidades con la intención y la capacidad del adversario, se pueden identificar las áreas de riesgo primario sobre las cuales enfocar los esfuerzos defensivos propios.

Un ejemplo de ello es la visión que tienen los analistas y planificadores chinos, para quienes:

> ...la fuente de la eficacia militar de los Estados Unidos proviene de la capacidad de integrar sistemas de información militar y civil y aprovechar ese acceso global a la información en el combate. Para ello, este valor en tecnologías de la información es un multiplicador de fuerzas para los Estados Unidos y un centro de gravedad vulnerable, pues si el adversario fuese capaz de desbaratar dichas redes y acceder a la información, el efecto que se produciría, dejaría a las fuerzas de combate estadounidenses y a sus comandantes en un estado de parálisis[436].

---

434 República Argentina. Ministerio de Defensa; Estado Mayor Conjunto de las Fuerzas Armadas; PC 20 – 01; Planeamiento para la Acción Militar Conjunta Nivel Operacional; Ed 2015, P. 54.

435 Williams, Brett, T. Ten propositions regarding cyberspace operations Op. Cit.

436 Krekel, Adams, and Bakos, Patton. Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage. Op. Cit.

Como ejemplo de dicho análisis, Karaman y otros, presentan el siguiente cuadro[437]:

FIGURA 7: EJEMPLO DE ANÁLISIS DE FACTORES CIBERNÉTICOS[438]

Ciber Centro de Gravedad	**Capacidades críticas (CC)**
Sistemas e infraestructura de sistemas de información militar.	Implementar ciberataques contra los sistemas e infraestructura de sistemas de información por medios manuales (contratar a una persona para el uso de *malware* o utilizar un disco duro infectado con gusanos en esos sistemas).
	Infectar los sistemas de información militar del enemigo con virus informáticos, gusanos o *malware* para robar o reunir información (capturas de pantalla, pulsaciones de teclas y archivos) por infiltración en los sistemas o *spear fishing* mediante el uso de las redes sociales, fuentes abiertas de inteligencia (OSINT) e ingeniería social
	Implementar un *"Zero Day"* para explorar una base de datos, email y servidores conectados en Internet.
	Implementar ataques DDOS.
	Llevar a cabo actividades de guerra ciberelectrónica para obtener inteligencia electrónica de registros de frecuencia de sistemas de mando y control mediante sistemas de alerta e inteligencia aerotransportada o drones.
Vulnerabilidades críticas (VC)	**Requerimientos críticos (RC)**
Uso limitado de actividades de ciber inteligencia.	Reunir OSINT sobre sistemas e infraestructura de sistemas de información militar y sus requisitos del sistema mediante redes TOR o direcciones IP falsificadas.
Desafíos legales nacionales e internacionales (¿Es un acto de Guerra o no? Ambigüedad de las leyes y Reglas de Empeñamiento).	Elaborar un documento jurídico marco donde se definan claramente las actividades, tareas y funciones cibernéticas.

»

437 Karaman, Muhammer y otros; Cyber Operation Planning and Operational Design. Op. Cit.

438 Karaman Cyber Operation Planning and Operational Design; Op. Cit. Traducción propia.

»

Falta de especialistas cibernéticos talentosos y especialistas en los ámbitos de planificación de las organizaciones militares.	Revertir la ingeniería y múltiples criterios de análisis de algunos conocidos *malware* dirigidos a recopilar información de los sistemas que infectan.
Falta de una estrategia diseñada para alcanzar la política de seguridad cibernética nacional, falta de intercambio de información con instituciones, universidades y empresas de defensa.	Iniciar la colaboración entre universidades, instituciones civiles y empresas de defensa sobre investigación y desarrollo (I&D) en cibernética.
Falta de una clara definición de las tareas que deben realizar las instituciones al respecto de las actividades cibernéticas.	Formar un equipo de redes sociales que trabaje permanentemente en Facebook, Twitter, LinkedIn, Instagram y otras.
La falta de integración de unidades de guerra cibernética y de inteligencia y el dilema de qué trabajo deben realizar cada una que deriva en una limitada cooperación entre estas dos áreas funcionales.	Poseer una base de datos de vulnerabilidades nacionales y suficientes ciber expertos y contratistas.
Los desafíos legales.	Un gran número de computadoras *zombies* y *botnets*.
La dificultad en la integración e implementación, bajo un único mando, de actividades ciber electromagnéticas en el nivel táctico	Fuerte cooperación entre unidades de inteligencia cibernética.

El hecho de que muchos sistemas de apoyo de combate no utilizan redes seguras indica posibles puntos vulnerables a ataques cibernéticos. El número de sistemas de información que pueden ser atacados, la gama de vulnerabilidades que estos pueden llegar a tener, la gran cantidad de funciones de apoyo de combate que apoyan y las complicadas conexiones hacen difícil las evaluaciones de las misiones operacionales. A ello se le debe sumar el carácter evolutivo de las amenazas y vulnerabilidades en el ciberespacio, razón por la cual la tarea de encontrar adecuados planes de mitigación para todas las posibilidades es profusa[439].

439 Snyder, Don, Hart, George E., Lynch, Kristin & Drew, John G., Ensuring U.S. Air Force Operations During Cyber Attacks Against Combat Support Systems, Guidance for Where to Focus Mitigation Efforts, Disponible en: http://www.rand.org/content/dam/rand/pubs/research_reports/RR600/RR620/RAND_RR620.pdf

Asimismo, podrían existir otras vulnerabilidades como por ejemplo involucrar a personal desleal o contratistas del Estado que por motivos de venganza, rencor personal o avaricia roban activos sensibles de la organización o restringen su integridad - Snowden[440] es el arquetipo - o que por desconocimiento permiten el acceso a un hacker a pesar de no tener ninguna intención de efectuar ciberespionaje. Otras pueden encontrarse tanto en el software como en el hardware que se utiliza, especialmente si este último es importado[441], como así también en los cables de fibras ópticas que transportan la información.

Además de todo ello, las redes son críticas y son casi siempre vulnerables. Desconectarse no es la solución. Se debe luchar en defensiva atravesando el ataque. Las redes son esenciales en todo el espectro del conflicto. No obstante, ningún comandante podrá garantizar que sus redes no serán atacadas, o que, en caso de ataque, serán inexpugnables. Si bien se puede caer en la tentación de desconectar los equipos en caso de ataque (auto denegación de servicio), eso sería darle la victoria al atacante. Una defensa robusta de los sistemas cibernéticos de comando y control puede dar idea de superioridad y obligar a que el enemigo gaste más esfuerzo en el dominio cibernético que en el dominio físico.

Para Jason Rivera[442], de la misma manera que las líneas de comunicaciones marítimas pueden definirse como pasajes interoceánicos, canales principales y grandes puertos, las líneas cibernéticas de comunicación pueden considerarse como puntos críticos de intercambio de Internet, líneas de cable oceánicas de fibra óptica, instalaciones de enlace de satélites principales comunicación *uplink / downlink* (SATCOM) y los más suscritos proveedores de servicios de Internet del mundo (ISP).

En un nivel más micro, en el dominio cibernético, las líneas de comunicaciones cibernéticas pueden caracterizarse a través de complejas y diferentes distribuciones tales como *routers, switches,* servidores, y direcciones IP vinculadas a redes. Para la estrategia militar, al igual que el control de las líneas de comunicaciones marítimas, es fundamental y también lo debe ser el control de las líneas de comunicaciones cibernéticas. Por lo tanto, cualquier modelo de planeamiento que busque desarrollar una estrategia para llevar a cabo la guerra cibernética debe incluir como objetivo principal la necesidad de asegurar las líneas de comunicación cibernéticas, tanto físicas (cable de fibra óptica, SATCOM, ISPs, etc.) como lógicas (red de dominios, servidores, *routers*, etc.).

---

440 Edward Snowden, ex analista de inteligencia quien filtró información clasificada de la Agencia Nacional de Seguridad de Estados Unidos (NSA) y que vive exiliado en Rusia desde 2014.

441 Informes del Departamento de Homeland Security de los Estados Unidos muestran que se encontró malware dentro de un hardware importado de China. Un malware Zombie Zero fue implantado en el software de un escáner fabricado en China como parte de un ataque dirigido contra las industrias de transporte y logística. El escáner, en apariencias inofensivo, cuando era conectado a una red proporcionaba una plataforma para comprometer todo en la red, en este caso comunicándose con servers de comando y control ubicados en China. Disponible en http://journal.georgetown.edu/u-s-military-defense-systems-the-anatomy-of-cyber-espionage-by-chinese-hackers/ fecha de consulta 18 agosto 2016.

442 Rivera, Jason, A Theory of Cyberwarfare: Political and Military Objectives, Lines of Communication, and Targets, Disponible en: http://georgetownsecuritystudiesreview.org/2014/06/10/a-theory-of-cyberwarfare-political-and-military-objectives-lines-of-communication-and-targets/

El punto decisivo cibernético

Para Milan Vego[443], en la era de la información ha surgido un nuevo tipo de punto decisivo llamado arbitrariamente el *punto decisivo cibernético*[444].

> Debido a que las fuerzas militares modernas dependen cada vez más de diversos sistemas informáticos de información y comunicaciones, un oponente podría llegar a intentar penetrar, interrumpir, degradar y descabezar a varios elementos de estos sistemas, dentro del Teatro de Operaciones, desde muchos cientos o miles de millas de distancia o desde el espacio ultraterrestre. Uno de los puntos decisivos más críticos en un sistema informático es el denominado clúster de servidores[445], o sea un grupo de servidores en red, ubicado en un lugar. Dichos servidores son a menudo los proveedores de servicios de Internet y pueden ser paralizados parcial o incluso totalmente tanto físicamente como mediante ataques informáticos.
>
> Si el oponente se basa extensivamente en sistemas computarizados para el comando y control, inteligencia, o para las defensas aéreas del teatro, es posible atacar indirectamente su centro de gravedad a través de un ataque contra sus "puntos decisivos cibernéticos". Las redes de computadoras son, en muchos casos, similares a una red de transporte, razón por la cual, los planificadores podrían seleccionar un método de ataque que se centre en los nodos críticos o clave cuya destrucción o aniquilación tendría un efecto dominó sobre el funcionamiento de la red como un todo.

Otros puntos decisivos que podrían ser considerados en el diseño operacional suelen ser: alcanzar la superioridad cibernética en el área de operaciones, asegurar la integridad de los sistemas con las fuerzas amigas, influir cibernéticamente en el área de operaciones, o bien ganar la mente del adversario. Los sistemas de información computarizados en red, necesarios para la transferencia de datos críticos o de comunicaciones de C^2, también pueden ser puntos decisivos cibernéticos.

Las operaciones cibernéticas durante y después de la confrontación

Durante la confrontación, el comandante operacional debe centrar su preocupación en el qué hacer y no en el cómo hacerlo. Qué estado final, qué efectos, qué objetivos, qué tareas, qué capacidades y todos ellos enlazados por el cuándo, el dónde y el quién.

> Esto no quiere decir que no haya preguntas referidas al cómo en el nivel operacional, pero ellas son secundarias con respecto a las preguntas más críticas que son las relacionadas con el qué; si se formulan erróneamente, no importará qué tan bien se ejecuten las acciones tácticas. Así que es necesario pensar en grande el qué y poco en el cómo en el nivel operacional, pero teniendo en cuenta que ambos están

---

443 Vego, M.; Joint Operational Warfare Theory and Practice Op. Cit. P. IV -62.

444 Para Vego: "Existen puntos decisivos en cada nivel de guerra; en cuanto a su escala y su importancia, se pueden distinguir puntos decisivos tácticos, operacionales y estratégicos. Op. Cit. P. GL-7 (el subrayado es propio).

445 Un clúster de servidores se basa en la unión de varios servidores que trabajan como si de uno sólo se tratase. Optimizan los procesos internos mediante la distribución de la carga de trabajo entre los componentes individuales de los sistemas y agilizan los procesos informáticos aprovechando la potencia de varios servidores. Los servidores pueden conectarse de tal manera que parecen representar una sola fuente.

presentes; simplemente, que la escala debe inclinarse hacia las preguntas relacionadas con el qué[446].

Hoy en día los países son muy cuidadosos respecto del empleo de la guerra cibernética y por ello justamente evitan que cualquier uso de ella pueda ser considerado por el derecho internacional como un acto de guerra. Por tal razón, durante la confrontación[447] para usar el término de la PC 20-01[448], al utilizarse el modelo de acción – reacción - contra reacción, en el nivel operacional deberá considerarse, entre otras cosas, la reacción que una acción cibernética pueda llegar a tener sobre el público nacional e internacional, así como también sobre el adversario.

Lo que se confronta en este paso es la reacción inicial ante un ataque cibernético. Lo primero que se trata de identificar es la atribución, aunque lo correcto es analizar el impacto operacional. Los Estados Mayores tienden a concentrarse en la autoría de la intrusión, cuando lo más apropiado debería ser tratar de identificar el impacto operacional y resolver las medidas de contraataque necesarias para detener el ataque.

En el nivel operacional, debido a las características del "problema de atribución", puede ser casi imposible discernir la intención o incluso la identidad de un agresor cibernético, lo cual hace muy difícil discutir la guerra cibernética según un análisis estratégico convencional – como una acción por parte de un enemigo conocido utilizando determinados recursos conocidos para alcanzar metas específicas-.

La atribución tendría que ser la clave para entender el motivo del ataque y, por lo tanto, ser capaces de diferenciar entre un acto criminal y un acto de guerra en el espacio cibernético, lo cual es crucial para poder coordinar las respuestas nacionales e internacionales. Pero el reconocimiento no es un tema sencillo. Puede ser difícil distinguir entre los diferentes desafíos a la seguridad cibernética de cuándo es una guerra cibernética, o extremismo cibernético, o un delito cibernético o simples travesuras pues todos pueden utilizar similares "tácticas, técnicas y procedimientos". Puede ser difícil establecer más allá de cualquier duda técnica que el gobierno de un estado podría haber sido responsable de un ciberataque lanzado con medios informáticos privados desde territorio de un segundo estado empleando la infraestructura electrónica de un tercero – un producto conocido como "negación plausible", que se encuentra en abundancia en el espacio cibernético[449].

Si bien existen varios tipos de ataque cibernético, los más complicados, como la de-

446 Eikmeier; Dale C.; Waffles or Pancakes? Operational- versus Tactical-Level War Gaming Joint Force Quarterly 78; 3rd Quarter 2015; P. 51

447 En los EE.UU y países de la OTAN este paso se denomina Wargaming Confrontación (de los propios cursos de acción con las capacidades del enemigo) que se asimila al paso 4 del Método de Planeamiento MDMP o JOPES. Como su traducción es Juego de Guerra, en la Argentina se lo confunde con un tipo de ejercicio de cuadros sobre la carta.

448 PC 20-01; Planeamiento para la Acción Militar Conjunta Nivel Operacional; Op. Cit.

449 Cornish, Paul; Livingstone; David, Clemente, Dave and Yorke, Claire; On CyberWarfare; A Chatham House Report; P. 26; Disponible en: https://www.chathamhouse.org/sites/files/chathamhouse/public/Research/International%20Security/r1110_cyberwarfare.pdf.

tección de movimientos logísticos, o cantidades logísticas computarizadas, o datos de salud, pueden revelar que es todo el propio sistema el que está en peligro. La opción más inquietante es cuando se sustrae documentación y lamentablemente es la opción más común. Aquí se hace necesario determinar qué tipo de documentación se extrajo, y no concentrarse en cantidades de megabytes sustraídos o en quién pudiera haberlo hecho.

Detectado el ataque, la primera opción podría ser la de desconectar el servidor, lo cual, como ya se dijo, sería una forma de aceptar una derrota, además de interferir con el propio sistema de Comando y Control. Otra opción sería la de manipular la intrusión para transformarla en una fuente de desinformación para el enemigo. Las opciones dependerán del riesgo que el Comandante Conjunto decida aceptar.

Como fuera dicho anteriormente, los ataques contra las infraestructuras críticas conllevan un mayor grado de riesgo para el atacante si se afectan blancos fuera del Teatro de Operaciones o en el territorio del adversario. Lo que debería esperarse es un ataque contra las redes de una fuerza militar desplegada en el Teatro de Operaciones. Por ello, en la confrontación tendrá que tenerse en cuenta cuándo es beneficioso iniciar ataques cibernéticos para dañar las infraestructuras críticas del adversario y, de esa manera, distraer a sus líderes políticos, y cuándo es mejor limitar cualquier ciberataque a objetivos militares dentro del Teatro de Operaciones.

Las operaciones cibernéticas y las funciones operacionales

En la actualidad, todo Comandante utiliza para conducir, sincronizar e integrar las operaciones conjuntas, un conjunto de actividades y capacidades relacionadas que se denominan funciones conjuntas o funciones operacionales[450], las cuales están compuestas por seis grupos básicos: Comando y Control, Inteligencia, Fuegos operacionales, Movimiento y maniobra, Protección y Sostenimiento. Estas funciones operacionales – así denominadas por su semejanza con las funciones logísticas – son los aspectos que se comparan durante la confrontación o juego de guerra a partidos contrapuestos, paso 4 del método.

Esto resulta de fundamental importancia, porque concluida la confrontación, como lo señala el profesor Vego[451] "deberá estar en condiciones, de resolver correctamente la secuencia y sincronización no sólo de las fuerzas conjuntas sino también de las funciones operacionales, antes y durante una campaña".

Para Crowell, en las guerras del siglo XIX "la manera en la cual el comandante piensa sobre la secuencia y sincronización de las funciones operacionales o de comando respecto del espacio cibernético y de las ciberoperaciones será crucial para poder alcanzar el éxito de la campaña". Es por ello que sugiere las siguientes preguntas para cada una de dichas funciones[452] las cuales, obviamente, no son excluyentes:

- **Comando y control:** ¿Qué organización deberá adoptar la fuerza conjunta cuando se ejecuten operaciones cibernéticas? O, quizás más importante aún, ¿qué organi-

450 Zarza Leonardo Arcadio; Conducción Militar por Funciones De Combate; Revista "Visión Conjunta" Año 7 Nro. 13; 2015; P. 34

451 Vego. M. Joint Operational Warfare Theory and Practice. Op. Cit. P. VIII-3.

452 Crowell; R. "War in the Information Age: A Primer for Cyberspace Operations in 21st Century Warfare; Op. Cit.

zación deberá conformar el comandante cuando conoce que el adversario llevará a cabo operaciones cibernéticas contra su fuerza?, ¿cómo se trasmitirán los planes y las órdenes hacia arriba y abajo de la cadena de comando cuando el espectro electromagnético se encuentre perturbado o negado?, ¿cómo es posible contrarrestar el uso del espacio cibernético al adversario?, ¿Cómo debe organizar su comando un comandante para recibir sus mensajes antes que sus adversarios?, ¿en un entorno electromagnético perturbado o denegado puede el comandante operacional comunicarse con sus subordinados y superiores? ¿Puede ser contrarrestado el mando y control del adversario?, ¿es necesario modificar las Reglas de Empeñamiento?

- **Inteligencia:** ¿Qué hace un comandante cuando su equipo de fuerzas especiales está realizando reconocimiento estratégico y él no puede comunicarse con ellos vía espacio cibernético?, ¿cuánta información clasificada es almacenada en una computadora o se mueve a través del espacio cibernético?, ¿cuánto conocimiento sobre las fuerzas propias tiene el adversario obtenido a través de la observación, investigación, análisis y comprensión del espacio cibernético?
- **Fuegos operacionales:** ¿Qué sucedería si el GPS es degradado o negado?, ¿qué otras opciones tendría, como comandante, para batir a los blancos?, ¿puede utilizar el espacio cibernético para facilitar o realizar fuegos operacionales, ya sea por él o por su adversario?, ¿debe darse en todos los casos una respuesta a un ataque cibernético o habrá situaciones donde convendrá permanecer en contacto para llevar a cabo una operación de vigilancia y de esa manera comprender su actitud o si fuese posible controlar sus acciones?
- **Movimiento y maniobra:** En un entorno electromagnético perturbado o interrumpido, ¿cómo navega en el mar o en el desierto si no funciona el GPS?, ¿cómo el hecho de utilizar software comercial sin clasificar, similar a los que utilizan las empresas de mensajería (FEDEX y UPS) puede afectar el seguimiento de los envíos de la carga militar y la recepción de esta en un puerto o aeropuerto de desembarque?, ¿qué decisiones debería tomar el comandante cuando le informan que partes significativas de su poder de combate se ha enviado a otro destino, debido a una intrusión de un hacker?
- **Protección:** ¿Necesita un comandante pensar en la protección de sus fuentes militares y no militares de la energía?, ¿pueden ser manipulados los datos en los sistemas informáticos propios por fuentes externas?, ¿qué sucede cuando las decisiones se demoran o no se puede utilizar la ventaja tecnológica de que se dispone?, ¿qué sucede cuando se advierte que el adversario, al cual se le asignaban reducidas capacidades tecnológicas, posee tecnología UAS y munición de precisión guiada y la utiliza para colectar inteligencia o atacar?, ¿qué pasa con los hackers para acceder a sitios de la web "*mil ar*"?, ¿sería útil saber qué tipos de manuales de entrenamiento en explosivos o armas biológicas disponen las tropas de su adversario?, ¿cómo se neutralizarían dispositivos explosivos improvisados controlados por radio?
- **Sostenimiento:** ¿Qué medidas deberán adoptarse para el seguimiento de los abastecimientos en el caso de que los equipos de cómputos de datos no funcionen?

El Teniente Coronel William S. Angerman[453] propone que el Comandante del Teatro estructure las operaciones cibernéticas alrededor de cuatro conceptos: *penetración y control del espectro, protección cibernética y fuegos operacionales, coalición virtual y mensajería cibernética,* a fin de dominar el espectro en el momento y lugar que él elija, en consonancia con su enfoque operacional y su intención.

La Penetración y Control del Espectro tiene dos elementos relacionados entre sí dentro de las consideraciones de tiempo y espacio de las operaciones. La Penetración se refiere a la capacidad de la fuerza para llevar a cabo las actividades cibernéticas con eficacia en el espectro del área de responsabilidad. El Control se refiere a la necesitad del Comandante de dominar, manejar o influir en el espectro en apoyo a una acción específica.

Protección cibernética (operaciones cibernéticas defensivas) y Fuegos[454] (operaciones cibernéticas enfocadas hacia el exterior) para Angerman[455] *"son dos caras de una misma moneda"*. Un Comandante deberá combinar la capacidad de protección cibernética de las fuerzas amigas con una capacidad ofensiva para degradar las del enemigo.

El área de Coalición Virtual aborda el tema de compartir la información de manera segura, flexible y manejable dentro de la coalición. El término coalición virtual pretende describir el intento del Comandante de intercambiar información y conocimientos para maximizar la unidad de esfuerzo hacia los objetivos.

En lo que respecta a la Mensajería Cibernética, Angerman sostiene que:

> El Comandante debe entender e influenciar las percepciones de las fuerzas propias, de los neutrales y del enemigo, mediante un acceso y empeñamiento proactivo a los medios digitales. No se trata de manipulación de datos, sino que se refiere a estar atento y consciente de lo que sucede con las comunidades online y aprovechar positivamente el poder de respuesta y resonancia que tienen los mensajes. Ganar la guerra de percepción es crucial para el éxito del Comandante, tanto en el propio país como en el extranjero. Mientras que las operaciones de información y comunicación estratégica tienen conceptos y procesos perfectamente establecidos, el mensaje estratégico del Comandante del Teatro deberá busca facilitar la velocidad, cobertura e impacto de sus mensajes en el mundo digital. La cantidad de medios digitales de comunicación que debería utilizar para influenciar tendría que ser la más amplia posible: cable noticias en la televisión (efecto CNN), Internet (blogs, You Tube, comunidades en línea), los medios sociales (Twitter) y tal vez incluso personales (mensajes de texto a teléfonos seleccionados).

---

453 Angerman, William S.; Cyber Power for the Joint Force Commander: An Operational Design Framework; National Defense University; Joint Forces Staff College; Joint Advanced Warfighting School; P. 40; Disponible en: http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA603670.

454 Angerman utiliza el término "fuegos para ser consistente con la terminología de las funciones operacionales o funciones de combate. El término "enfocadas hacia el exterior" lo utiliza en lugar de "ofensiva" pues estas operaciones podrían suponer vigilancia u otras preparaciones de acceso cibernético que no son necesariamente ofensivas o destructivas.

455 Ibidem: P. 27

FIGURA 8: CUADRO DE IMPLEMENTACIÓN DE LAS ÁREAS CIBERNÉTICAS[456]

JFC Cyber Focus Areas	Spectrum Penetration & Control	Cyber Protection	Cyber Fires	Virtual Coalition	Strategic Cyber Messaging
	Operational Cyber Capabilities Available to JFC in Operational Design				
Cyber Decisive Points	*Spectrum Superiority in JOA*	*Cyber Integrity of Friendly Forces and Systems*	*Cyber Influence in JOA*	*(JFC Force Synergy) Coalition Situational Awareness, C2, and Information Sharing*	*(Win the info war) (Win hearts/minds) Resonate JFC Messages in JOA*
Cyber Functional Capabilities for Integration by Phase and with other Joint Functions within the Operational Design	(Phase I-IV): Collect adversary signals (***Intel***)	(Phase 0-V): Identify critical systems and access for JFC ops (***Intel, Protect***)	(Phase I-IV): Perform adversary system ISR (***Intel***) (Clandestine)	(Phase I-V): Allow partner contributions and access levels (***M&M, Sustain***)	(Phase I-III): Persuade key decision makers (***C2, Intel, Fires***)
	(Phase I-V): Deliver coalition frequency interoperability (***C2***)	(Phase 0-V): Provide situational awareness of system readiness (***Intel, Fires, Protect***)	(Phase I-IV): Shape JOA for joint operations (***All***) (Clandestine)	(Phase I-V): Share Coalition information securely (***Intel, Protect, M&M***)	(Phase I-III): Intimidate adversary force (***Intel, Fires***)
	(Phase I-V): Ready multi-spectral broadcasts (***C2, Fires***)	(Phase 0-V): Ensure redundancy of systems (***Protect***)	(Phase I-V): Leverage JOA data mining (***Intel***)	(Phase I-V): Promulgate and coordinate C2 activities (***C2***)	(Phase I-V): Disseminate information to wide audience (***M&M***)
	(Phase I-V): Extend Single Integrated Network Environment for coalition JOA ops (***All***)	(Phase 0-V): Protect and guarantee critical system availability and reliability (***All***)	(Phase II-III): Deny adversary service (***Fires***)	(Phase I-V): Facilitate JOA coalition planning & interoperability (***All***)	(Phase I-V): Shape coverage/ content of news cycle (***Intel***)
	(Phase II-III): Jam adversary systems (***Fires***)	(Phase 0-V): Protect friendly systems (e.g. passwords, firewalls, anti-virus) (***Protect***)	(Phase II-III): Deceive adversary (***Intel***) (Clandestine)	(Phase II-IV): Synchronize coalition joint force operations (***C2, Intel, Fires, M&M***)	(Phase I-V): Identify audience; target persuasive arguments & commitments (***Intel, Fires***)
	(Phase II-III): Mislead; spoof JOA activity/ signals (***Intel***) (Clandestine)	(Phase 0-V): Identify/marginalize cyber threats and manipulation (***Intel, Protect***)	(Phase II-III): Manipulate adversary data (***Intel, Fires***) (Clandestine)	(Phase II-V): Decentralize real-time JOA situational awareness & decision support (***Intel***)	(Phase I-V): Garner public support in JOA (***Intel, Fires***)
	(Phase II-III): Control JOA spectrum for decisive joint ops (***C2, Fires, Protect, M&M***)	(Phase 0-V): Reconstitute cyber capabilities (***All***)	(Phase II-III): Degrade/delay adversary capability (***Fires***)	(Phase IV-V): Provide system resources for population/civil authorities (***C2, Sustain, M&M***)	(Phase I-V): Reinforce JFC messages and talking points (***Intel, Fires***)
	(Phase II-V): Protect/amplify/ repeat friendly signals in JOA (***C2, Fires, Protect, M&M***)	(Phase I-IV): Accelerate response to denial of service (***C2, Protect, M&M***)			
	(Phase II-IV): Deny adversary spectrum/signals (***Fires***)				

Joint Functions Key: **C2** – Command & Control; **Intel** – Intelligence; **Fires** – Fires; **Protect** – Protection; **Sustain** – Sustainment; **M&M** – Movement & Maneuver

456 Fuente: Angerman; William S.; Cyber Power for the Joint Force Commander: An Operational Design Framework Op. Cit. P. 40.

Para lograr todo ello, Angerman propone un cuadro (Figura 8) para mejorar y equilibrar las relaciones entre el *JFC y USCYBERCOM*, el cual bien podría ser adaptado para establecer las relaciones entre un Comandante de Teatro y un Comandante Conjunto de Ciberdefensa.

La propuesta proporciona una visión y una estructura de la organización del Estado Mayor del Comando del Teatro, lo cual le permitiría al Comandante no sólo identificar y requerir objetivos cibernéticos y efectos deseados localizados, sino también aprovechar la esfera de la información para alcanzar superioridad de la información/cibernética y crear condiciones beneficiosas en todos los dominios del espacio de batalla.

Por último, en lo que respecta al tempo de las operaciones, el Comandante deberá considerar la cantidad de tiempo que le demandaría identificar, evaluar y penetrar un determinado objetivo, especialmente si las redes o el software se cambian con frecuencia, el cual podría llegar a superar cualquier línea de tiempo bajo la cual debe operar.

Reglas de empeñamiento en las operaciones cibernéticas

En el ciberespacio, el conocimiento de la situación puede llegar a ser realmente dificultoso pues los Comandantes de un Teatro de Operaciones, por lo general, no tienen las herramientas confiables para identificar, controlar y estimar un ataque, ni disponen de equipos sofisticados para identificar y rastrear los flujos de información hostil.

Tampoco están definidas las reglas de empeñamiento (RDE) para los operadores de redes durante los ataques cibernéticos. ¿Cuándo el espacio de batalla es cibernético, en qué condiciones un operador puede "devolver el fuego" cuando recibe ataques activos y hostiles? ¿Cuándo el comandante de un centro de operaciones de red puede instruir a sus subordinados para proyectarse dentro del Teatro de Operaciones cibernético? ¿Cuáles serían las reglas de empeñamiento en ese caso? ¿Qué situaciones infieren qué contramedidas? ¿Cuándo un ataque cibernético (o amenaza de ataque cibernético) da lugar a ejercer el derecho de defensa propia — lo que incluye la defensa propia armada, entendiéndose por "ataque cibernético" el uso de códigos informáticos maliciosos o señales electrónicas para alterar, perturbar, degradar o destruir sistemas informáticos o redes de información?

Un primer aspecto a tener en cuenta es saber distinguir entre espionaje en línea y ataques militares, una división que puede ser borrosa en la práctica. Por lo general, se trata de bloquear e impedir un ataque poniendo énfasis en la defensa y la negación de acceso a los atacantes. En caso de que ello fallase, el siguiente paso sería la "defensa activa", con una "respuesta proporcional" de contraataques contra el agresor.

Como se ha visto a lo largo de esta investigación, resulta muy difícil, utilizando medios puramente tecnológicos, rastrear el origen de algún tipo de ataque, pues, no se puede sólo mirar la conexión entre un computador y otro porque los ciberatacantes utilizan varios niveles de servidores que hacen difícil determinar de dónde se envían los datos. Estos equipos, por lo general, están fuera del Teatro de Operaciones por lo que hay posibilidades de solicitar los archivos de registro de los equipos, como ocurría con un ciberdelito relacionado con la pornografía infantil, etc.

Funcionarios y expertos en seguridad cibernética todavía están debatiendo cómo definir los diferentes tipos de ataques cibernéticos y cómo determinar una respuesta proporcional.

Dado que el ciberespacio es un ámbito que se extiende más allá de la jurisdicción de cualquier nación, que las operaciones de redes de computadoras son la principal forma de operaciones en el ciberespacio, y con frecuencia son no cinéticas, la determinación de actos hostiles e intentos hostiles se ve dificultada. Además, el espacio cibernético presenta desafíos únicos, como la capacidad de los actores de mantener la "negación plausible", que hace sumamente difícil definir quién está detrás de un ataque.

Para Brian T. O'Donnell y James C. Kraska[457]

> ...a diferencia de una granada de mano, el ataque de red de computadoras podría tener diferentes efectos dependiendo del sistema contra el que se lanza. Además, en la medida en que la tecnología cambia, puede ser que el ataque no tenga el mismo efecto previsto originalmente. También es motivo de preocupación, debido a la complejidad de los principios de la programación, ¿cómo el comandante de teatro puede alcanzar el mismo nivel de comprensión que los expertos en informática?, ¿puede confiar en el juicio de otro cuando él es quien debe "apretar el gatillo" ?, ¿cuál es el mínimo nivel de conocimientos que el comandante debe poseer?"

Como ya ha sido explicado en este trabajo, las redes y sistemas de computadoras son complejas, interactúan de diferentes maneras y pueden tener interdependencias imprevistas que produzcan efectos colaterales que son difíciles de evaluar *ex ante*. Un ejemplo famoso es el ataque que llevó a cabo en 2008 el Pentágono contra un foro utilizado por los extremistas en Irak, que causó inadvertidamente las interrupciones de la Internet en Arabia Saudita y en Texas[458]. ¿Habría sido posible anticipar las interrupciones por adelantado? Si es así, ¿qué consideraciones debieron utilizarse para evaluar las ventajas de la operación vis a vis el daño esperado?

Seguramente, requerirá la inversión de significativos recursos de inteligencia antes de llevar a cabo una operación de una determinada topología de red y aprender sobre los tipos de interdependencias que existen; ¿es factible en el caso de los ataques cibernéticos más planificados este tipo de uso intensivo de recursos para llevar a cabo esa evaluación?

Es por eso que para O'Donnell y James C. Kraska un Comandante debe, al menos:

- ¿entender qué hace el objetivo y cómo funciona?
- ¿comprender cómo y qué hará al sistema de destino una operación de defensa activa?

---

457 O'Donnell, Brian T. & Kraska, James C. International Law of Armed Conflict and Computer Network Attack: Developing the Rules of Engagement, International Law Studies, Vol 76. P.

458 Romanosky, Sasha & Goldman, Zachary K. What Is Cyber Collateral Damage? And Why Does It Matter? Tuesday, November 15, 2016, 1:30 PM, Disponible en: https://www.lawfareblog.com/what-cyber-collateral-damage-and-why-does-it-matter

- ¿estar en posición de juzgar, ya sea por inteligencia u observación directa, los efectos del ataque?
- determinar ¿qué otros sistemas comparten o están relacionados con el sistema del objetivo, ¿cómo funcionan y qué controlan?

Para el Manual de San Remo[459], las principales consideraciones legales al hacer el borrador de las Reglas de Empeñamiento para operaciones en el ciberespacio son:

I. Las políticas nacionales y las leyes criminales y civiles domésticas e internacionales varían mucho en los aspectos legales de las operaciones de red de computadoras. Aún más, los tratados de comunicaciones multilaterales y bilaterales tienen provisiones que impactan la conducta de las operaciones de redes de computadoras.
II. A pesar de que no son cinéticas, las operaciones en el ciberespacio pueden constituir un acto hostil o un intento hostil. Los factores en la determinación de ambos incluyen la severidad, rapidez, lo directo y los efectos de la operación.

Sobre la base de lo hasta aquí expresado se desprende la necesidad de establecer algunos principios prácticos para el desarrollo de reglas de empeñamiento, la forma de determinar los posibles daños colaterales y su aplicación por parte de los comandantes de teatro y de fuerzas de tareas conjuntas. No obstante, en el anexo al final del trabajo se podrán ver algunos tipos de reglas de empeñamiento para operaciones cibernéticas.

Conclusiones del capítulo

En la actualidad, los límites entre los diferentes niveles de la guerra en la gama de operaciones militares están desdibujados, pero en las operaciones cibernéticas pareciera ser que lo están aún más.

Sean o no las operaciones cibernéticas de una dimensión estratégica, debe reconocerse la gran importancia que tiene el hecho de llevar a cabo operaciones en el espacio cibernético.

Cualquier potencial objetivo teóricamente podría ser estratégico, operacional o táctico, según el propósito para el cual es utilizado y por quién. Dado que resulta engorroso asignar a un blanco su calidad de estratégico, operacional o táctico, es importante examinar los tipos de efectos que se pueden crear en un ataque cibernético y sus consecuencias.

Como el espacio cibernético es un dominio hecho por el hombre, difiere de los otros de aire, mar, tierra y espacio. Históricamente, los principios de la guerra convencionales del Mariscal Foch se aplican a cada dominio, por separado, y al campo de batalla, en su conjunto. El espacio cibernético contrasta con los otros dominios porque, como se ha visto, muchos de esos principios no se aplican, o se aplican en forma diferente dentro de la guerra en redes. No obstante, los esfuerzos en el espacio cibernético contribuyen a la

459 Instituto Internacional de Derecho Humanitario, Manual de Reglas de Enfrentamiento, San Remo, noviembre 2009, P. 15

aplicación de los principios de la guerra a través del campo de batalla y, por otra parte, en el espacio cibernético existen principios doctrinarios con respecto a la dirección estratégica, al arte operacional y al comando y control de las operaciones análogos a los empleados en las operaciones de los dominios territoriales. "En lo único que hay que cuidarse es en las analogías erróneas que por simplistas pueden llevar a error"[460].

Establecer un perfil psico-social del potencial enemigo, determinar su intención, objetivo, ubicación, movimiento, estado, capacidad, estructura de apoyo, adquirir una comprensión exacta de la infraestructura, los sistemas y la dinámica del entorno de sus redes de computadoras y su impacto en las operaciones permitirá identificar los componentes clave y sus tecnologías y, por ende, sus vulnerabilidades.

Al descubrir las vulnerabilidades del enemigo antes de un conflicto, un comandante operacional puede integrar los ataques a redes de computadoras en forma rápida y sorpresiva con operaciones coordinadas en otros dominios.

El tiempo afecta a las operaciones en el espacio cibernético mucho más que en los otros dominios. La preparación de un ataque a una red de computadoras ocurre antes de que se inicie un conflicto mediante espionaje y análisis de red de forma tal que cuando comience la conflagración, el comandante pueda usar las opciones del espacio cibernético inmediatamente. Todas las operaciones cibernéticas preparatorias a los enfrentamientos entran en la categoría de operaciones cibernéticas del nivel operacional.

La aplicación de la fuerza en el espacio cibernético se diferencia de los otros dominios de aire, mar, tierra y espacio. La fuerza en el espacio cibernético puede lograr resultados similares en los otros dominios minimizando los daños físicos en los blancos. Si se inhabilita un nodo de comunicaciones de un enemigo con un virus, ello niega su uso al enemigo de la misma forma que si hubiese sido destruido por una bomba. No obstante, el uso de un ataque a una red de computadoras hace que la reparación de ese nodo sea más barata y más rápida que la destrucción cinética del nodo. Así, tomar ventaja del espacio cibernético permite que el Comandante Operacional logre efectos similares, pero causando menos destrucción que las opciones convencionales.

Es por ello que los actuales principios de la guerra parecieran necesitar de una considerable ampliación y revisión, lo cual no significa que deban ser descartados. Todos los actuales principios de la guerra convencional surgieron luego de siglos de experiencia y representan elementos esenciales, atemporales, de una guerra que seguirá siendo relevante en el futuro, aunque la mayoría son aplicables ahora en circunstancias más limitadas.

Dado que a lo largo de esta investigación se ha podido apreciar que las guerras en el futuro serán una mezcla de enfrentamientos convencionales, insurgencias y ciberataques es que se considera que los actuales principios deben ser convertidos en otros más complejos que representen un mejor enfoque para el futuro. Por estas razones, los principios de la ciberguerra son, en última instancia, diferentes de los de la guerra cinética y *más aplicable a las guerras híbridas.*

---

460 Williams, Brett T; Ten propositions Regarding Cyberspace Operations. Op. Cit. P. 61.

En lo que respecta a la inclusión de las operaciones cibernéticas de defensa activa en el planeamiento de una campaña, se considera que las mismas deberían conceptualmente ser consideradas como una suerte de "fuegos operacionales" por cuanto su grado de letalidad puede adaptarse a la situación, ser (al menos en algunos casos) reversible y resultar menos costosas que otros métodos de búsqueda de efectos similares.

No obstante, los comandantes operacionales deberían centrarse predominantemente en las operaciones defensivas pasivas del espacio cibernético, limitar su capacidad activa para una defensa cibernética dinámica y contraataques y no atacar preventivamente en el espacio cibernético. Las operaciones cibernéticas ofensivas deberían quedar en manos de la estrategia militar.

Se afirma entonces que restringir las capacidades y las operaciones cibernéticas a las puramente defensivas cederá la iniciativa al oponente. Ello obligará a quien se defiende a adoptar una postura reactiva, estratégica, operacional y tácticamente. Contra lo que la intuición pareciera indicar, una mejor defensa requerirá del conocimiento de capacidades ofensivas para poder detectar e interrumpir los ataques antes de que estos causen daños inesperados.

Hasta el presente, la mayoría de los ataques cibernéticos han producido efectos intangibles, ampliando la "niebla de guerra" creando indecisiones y retardando las reacciones de los oponentes. Los sistemas de armas modernos dependen de un software cuya alteración puede dañar su rendimiento. Manipular la opinión pública para dañar la legitimidad y autoridad de un oponente entre el público nacional e internacional puede ser también un objetivo que algunos antagonistas probablemente traten de perseguir.

Los ataques cibernéticos pueden ser moderadamente destructivos, rápidos y baratos, pero nadie desarrollaría un plan de campaña utilizando sólo armas cibernéticas. Estas no son tan destructivas como para dañar la voluntad y capacidad para resistir de un oponente. Los ataques cibernéticos no son decisivos, particularmente contra un rival grande y poderoso. La amenaza de represalias que se limita a una respuesta cibernética también puede no ser muy convincente.

La capacidad de alterar las redes, sistemas de armas y de comando y control puede proporcionar una ventaja significativa en combinación con otras armas. Sin embargo, las opiniones difieren respecto de si es posible construir medios cibernéticos ofensivos, durante el planeamiento y la ejecución de las operaciones, que, además, sean discretos y oportunos.

Las operaciones de guerra en el espacio cibernético se caracterizan a menudo porque el adversario es siempre ambiguo, el entorno de Internet es anónimo y no es fácil predecir el posible impacto negativo de los efectos de segundo y tercer orden[461] en relación con el objetivo principal. En el espacio cibernético, la naturaleza del objetivo no es fácilmen-

461 El efecto de primer orden es el impacto directo de la actividad cibernética en los datos de la computadora destino. Ello produce un efecto de segundo orden que afecta el servicio que presta el equipo de destino. Los daños, lesiones u otras consecuencias que provocan la terminación o interrupción del servicio a los clientes del sistema informático constituyen los efectos de tercer orden, que bien pueden haber sido el objetivo principal en el desarrollo de la operación cibernética.

te comprensible y por lo tanto requiere de un análisis minucioso. Ello demanda tiempo y esfuerzo que no siempre coincidirán con el *tempo* de las operaciones.

Por lo tanto, se hace necesario tener que abordar las características pertinentes a los objetivos que son de interés operacional y táctico, área aún poco explorada, debido a que muchas de estas características están alineadas, al menos en parte, con las competencias tradicionales de las áreas de inteligencia y guerra electrónica.

Debido a su sensibilidad y a la asignación actual de las competencias, las capacidades ofensivas cibernéticas existentes se han desarrollado casi exclusivamente en programas altamente clasificados. Quienes argumentan que, si se tratara de tomar la decisión de aprovechar las capacidades ciberofensivas más enteramente en los niveles inferiores de la guerra, ello no podría ser efectivamente realizado manteniendo el nivel de clasificación de seguridad necesario. Por otro lado, si el conocimiento de las capacidades de las armas cibernéticas quedara restringido a un nivel superior del Comandante del Teatro al que este no estuviera autorizado a acceder, no se podrá pretender que ese Comandante considere su uso en la planificación y la ejecución de una campaña. De tenerlo, ese Comandante podría llegar a tener mejores opciones para cumplir con su misión, como por ejemplo, desactivar un sistema de defensa aérea que podría no haber querido atacar con armas convencionales porque se encuentra deliberadamente colocado cerca de un hospital o cerca de un puente estratégico importante.

El Comando Conjunto de Ciberdefensa resulta hasta el momento, el que en mejores condiciones se encontraría para coordinar los efectos ciberespaciales deseados contra un blanco, basado en las prioridades del Comandante del Teatro o del Comandante de la Fuerza de Tareas Conjunta.

Sin perder la capacidad de planificar y dirigir operaciones militares convencionales, los desafíos que presentan los conflictos modernos, así como las nuevas modalidades de empleo de las fuerzas militares, indican la necesidad de formar oficiales para que sean capaces de actuar en ambientes operativos muy diversos y exigentes, en los que no solo deben usar su intelecto, sino también ser capaces de trabajar bajo la presión de la ambigüedad y de asumir acertadamente iniciativas.

Los conflictos actuales claramente combinan nuevos actores con nuevas tecnologías y nuevas formas de la guerra, pero las viejas amenazas también permanecen y tienen que tratarse al mismo tiempo y en el mismo espacio.

El dominio cibernético tiene características que le son propias. Hay que evitar caer en tecnicismos, y pensar que solamente los hackers se desenvuelven en este ámbito. El Comandante de Fuerzas Conjuntas puede admirarse de la forma en que los hackers suben la escalera del éxito, pero es el Comandante de Fuerzas Conjuntas el que indicará "sobre qué pared deberá apoyarse la escalera".

El espacio cibernético es un dominio hecho por el ser humano, y la tarea que viene es darle forma para alinearlo con el ambiente operacional. Hasta que eso suceda, y hasta que los Comandantes de Fuerzas Conjuntas se familiaricen con los aspectos técnicos de Comando y Control, podrá delegar en sus asesores los aspectos que aseguren su libertad de maniobra en el espacio cibernético. De cualquier forma, siempre retendrán la responsabilidad.

CAPÍTULO 6

EL EMPLEO DE LAS CAPACIDADES CIBERNÉTICAS EN APOYO DE LAS OPERACIONES DE INFORMACIÓN

Introducción

El diálogo de los medios es citado con frecuencia por los politólogos y diplomáticos como un clásico caso de estudio del realismo político. Llevado a cabo durante las negociaciones entre los emisarios atenienses y los gobernantes de Melos, una colonia de Esparta, los atenienses exigieron que su oponente se rindiera y pagara los correspondientes tributos a cambio de no ser destruida. Los atenienses no deseaban discutir sobre la moralidad de la situación, porque en la práctica sabían que la justicia dependía de la capacidad de coerción o, en sus propias palabras, del hecho *"que el fuerte hace lo que puede hacer y el débil acepta lo que debe aceptar"*[462].

El hackeo de los correos electrónicos del Comité Nacional Demócrata de Estados Unidos ampliamente atribuido a la inteligencia rusa, lo que mostraba el intento de intervenir en una elección presidencial de Estados Unidos y la negación frente a la creciente evidencia de la complicidad del gobierno de ese país motivaron a los analistas a hacerse una serie de preguntas, como, por ejemplo: ¿por qué el gobierno ruso haría algo así? Para Eugene Rumer[463] la respuesta es simple: "...porque puede hacerlo. El conocimiento es poder".

Esta respuesta parecería convalidar el axioma antes mencionado según el cual, el verdadero poder siempre recaería en aquellos Estados con un poderío militar considerable y quizás por esa razón, entre otras, en el año 2003, en ocasión de la segunda invasión a Irak, el presidente de Estados Unidos y la coalición conformada al efecto, llevaron a cabo una operación militar para desarmar a Irak de armas de destrucción masiva y bloquear el

462 Thucydides; History of the Peloponnesian War; Penguin Classics; Edic. 1972, P. 402

463 Rumer, Eugene B., The Kremlin's Advantage Why Cyberwar Will Continue, Foreign Affairs Snapshot August 2, 2016. Disponible en: https://www.foreignaffairs.com/articles/russian-federation/2016-08-02/kremlins-advantage.

supuesto apoyo de Saddam Hussein al terrorismo dirigido por Osama Bin Laden. Nunca quedó demostrada la existencia de tales armas, ni el apoyo del ex presidente iraquí al terrorismo, no obstante, la coalición lo destituyó, cambió al grupo árabe predominante en el gobierno y ajustició al líder iraquí tras un juicio shiíta en el año 2004.

Más aún, un año más tarde, el mundo, a través de la Organización de las Naciones Unidas asumió la "Responsabilidad de Proteger" (R2P). Esta doctrina sostiene que cuando un estado soberano no puede prevenir la comisión de atrocidades, los gobiernos extranjeros pueden intervenir para detenerlas formalizando un derecho de injerencia por el cual los Estados poderosos se arrogan el derecho de intervenir militarmente ante su apreciación personal de violaciones a los derechos humanos o al derecho internacional por parte de cualquier Estado. Así, y a propósito de esto, surge claramente que los Estados militarmente débiles están a merced de los más poderosos.

Bajo esa premisa se justificaron los bombardeos en Libia en 2011, por parte de algunos países occidentales, incluido los Estados Unidos. "La intervención militar internacional en Libia no es para imponer la democracia o matar a Muammar Qaddafi, Legal, moral, política y militarmente tiene sólo una justificación: proteger a la población del país."[464].

Sin embargo, frente a esta gran diferencia de poderío militar, tecnológico o de influencia diplomática, el más débil comenzó a utilizar, con mayor énfasis con que lo había hecho hasta ese entonces, cualquier método o clase de lucha, sin tener en cuenta siquiera, ninguna objeción ética.

Desde noticias para blogs, redes sociales y mensajería de texto, el rápido flujo de información ha cambiado la estructura social del mundo. La capacidad de las redes sociales en el espacio cibernético para incitar el apoyo popular y difundir la ideología no se limita geográficamente, y la continua proliferación de las TIC representa profundas implicancias para la seguridad nacional de los estados.

En la actualidad, los teléfonos inteligentes y dispositivos portátiles han transformado la forma en que gran parte del mundo se comunica e interactúa. En el presente, cualquier persona, mientras está en su trabajo, puede liderar una movida digital a miles y miles de kilómetros de distancia y generar un grito de tendencia mundial de millones de personas que simplemente operan desde sus *Tablets* y teléfonos inteligentes. Hay una nueva territorialidad. Semanalmente, una persona cualquiera puede usar entre diez o quince dispositivos conectados a Internet o basados en un algoritmo para realizar una tarea, según sea su conocimiento de la tecnología. Estos dispositivos pueden incluir *Fit - Bits*, teléfonos celulares, computadoras personales y/o de trabajo, sistemas de vigilancia caseros, GPS en el automóvil, televisión por Internet, impresoras, escáneres, tal vez una cafetera o un refrigerador. Es lo que se llama "la Internet de las cosas" (IoT)

La idea de la interconexión no es sólo acerca de la Internet de las cosas, sino también la información que transita en Internet y cómo influye en las decisiones diarias de las personas.

---

464 Jayshree Bajoria; Libya and the Responsibility to Protect; March 24, 2011; Council for Foreign Relations; Disponible en: http://www.cfr.org/libya/libya-responsibility-protect/p24480

Hoy, desde cualquier lugar del mundo, una vivienda particular, un bar, viajando en ómnibus, etc. la militancia y la lucha se dan en el mundo virtual. Así como la televisión provocó la idea de que "si algo no se televisa, no existe", con la llegada de las redes sociales el concepto mutó a "si el reclamo no es *trending topic*, no existe". Se utilizan "*call centers*" para impulsar consignas en las redes sociales o atacar al adversario, cualquiera que sea. La profesionalización es cada vez más grande.

Los ciberoperadores siguen con atención los nichos de micro militancia y bajada de línea de los adversarios. Hay una cuenta en particular que nutre de información y "*argumentos de discusión*", como ellos mismos dicen, para debatir con los opositores. Pero no es en Twitter, Facebook o Instagram. Es en *Telegram*, un servicio de mensajería como *WhatsApp*, con la posibilidad de crear "*canales de difusión*", donde los usuarios se pueden suscribir y recibir información.

A su vez, para evitar ser detectados, en vez de concentrar sus esfuerzos en un medio, los usuarios promueven mensajes a través de varias plataformas, asegurándose, de esa manera, la supervivencia digital si una cuenta es suspendida.

Hasta hace poco tiempo atrás, el uso de las computadoras raramente se extendía más allá del apoyo a determinadas funciones de combate[465]. Las funciones de combate, según Zarza, son el conjunto de actividades y capacidades relacionadas que todo Comandante utiliza para conducir, sincronizar e integrar operaciones conjuntas. En todos los niveles de conducción de una guerra las funciones de las operaciones militares, comunes a toda operación conjunta están compuestas por seis grupos básicos: Comando y Control, Inteligencia, Fuegos, Movimiento y maniobra, Protección y Sostenimiento.

Hoy, como se verá a continuación, abarcan mucho más. "Hoy en día, los mapas no pueden describir un campo de batalla en el cual el enemigo puede subir un video para una audiencia de millones de personas desde cualquier casa en cualquier suburbio de cualquier ciudad."[466]

Las operaciones de información en las doctrinas militares

Las operaciones de información buscan desinformar para hacer confundir al adversario en su toma de decisiones, o influir en la mente de este para cambiar sus actitudes. Asimismo, y como podrá apreciarse en este capítulo, las computadoras y redes de computadoras son una herramienta más en esta clase de operaciones militares.

Las operaciones de información buscan negar o manipular el proceso de toma de decisiones de un adversario o potencial adversario, atacando un medio de información (como por ejemplo un punto de acceso inalámbrico en la dimensión física), el mensaje en sí mismo (un mensaje cifrado en la dimensión de la información), o una ciber-persona (una identidad en línea que facilita la comunicación, toma de decisiones y la influencia de las audiencias en la dimensión cognitiva). A diferencia de otros efectos que se pretenden alcanzar en el campo de batalla, se centran en tratar de influir en

465 Zarza, Leonardo Arcadio; "Conducción Militar por funciones de Combate" Revista de la ESGC Visión Conjunta Buenos Aires, Argentina, N° 13, P. 33

466 McChrystal, Stanley; Teams of Teams: New Rules of Engagement for a Complex World, Portfolio/Penguin, 2015; P. 25 El autor fue Tte. Gral. Retirado del Ejército de los Estados Unidos.

las percepciones o actitudes de quienes deben tomar decisiones en lugar de destruir cosas o ganar terreno.

Desde que, en 1998, el US Joint Chiefs of Staff promulgó la Joint Publication JP 3-13, "*Joint doctrine for Information operations*"; estas operaciones han incluido medidas ofensivas y defensivas para manipular la información enemiga y sus sistemas de información, así como los procesos de toma de decisiones, y también para defender la información, sistemas de información y procesos de toma de decisiones propios. Estas operaciones incluyen una amplia gama de conceptos como guerra psicológica, la destrucción física, guerra electrónica, ataques contra redes de computadoras y la defensa contra tales, el engaño militar, contra propaganda, contra engaño, seguridad de la información, seguridad operacional, intrusiones y ataques informáticos.

Para los Estados Unidos[467], las operaciones de información se caracterizan por el empleo integrado, durante operaciones militares, de herramientas, técnicas o actividades utilizando datos, información o conocimiento para crear efectos y condiciones operacionalmente accesibles dentro de las dimensiones físicas, de información y cognitivas del entorno de la información, en concierto con otras líneas de operaciones, para influir, alterar, corromper o usurpar la toma de decisiones de adversarios y potenciales adversarios protegiendo, al mismo tiempo, las propias.

Existen muchas capacidades militares que contribuyen a las operaciones de información que deben tenerse en cuenta durante el proceso de planificación. Estas incluyen: comunicación estratégica, grupos de coordinación interinstitucional, asuntos públicos, operaciones civiles y militares, ciberoperaciones, seguridad de la información, inteligencia, engaño militar, seguridad de las operaciones, operaciones técnicas especiales y operaciones en el espectro electromagnético conjunto.

Para la doctrina militar de la República Federativa de Brasil[468] las Operaciones de Información,

> ...son operaciones coordinadas que contribuyen al logro de objetivos políticos y militares. Se ejecutan con el propósito de influir en un opositor real o potencial, disminuyendo su capacidad de combate, cohesión interna y externa y su capacidad de toma de decisiones. Actúan en los campos cognitivos, físicos e informativos de la información del oponente[469] y también en los procesos y los sistemas por los que viajan, al mismo tiempo en que buscan proteger a las fuerzas amigas y sus respectivos procesos y sistemas de toma de decisiones"[470].

---

467 Joint Publication 3-13; Information Operations; 27 November 2012 Incorporating Change I; 20 November 2014. Disponible en http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf.

468 Las Operaciones de Información, en la actualidad incluyen a las operaciones de inteligencia, de guerra electrónica, el engaño militar, las operaciones de seguridad y las operaciones psicológicas, el ataque físico y el ataque por red informática.

469 El resaltado es propio.

470 Brasil. Ministério da Defesa; GLOSSÁRIO DAS FORÇAS ARMADAS; MD 35-G-01; 4a Edição 2007; P. 183/274 Disponible en http://www.defesa.gov.br/arquivos/File/legislacao/emcfa/publicacoes/md35_g_01_glossario_fa_4aed2007.pdf

Gabriel Barbeito, expresa que[471]:

> Si bien no hay una única definición para las operaciones de información, se puede acordar que son acciones que implican el uso y manejo de tecnología de la información y la comunicación para acceder, modificar, interrumpir, alterar o destruir la información del oponente en procura de obtener una ventaja competitiva, así como asegurar la integridad de la información propia.

Para el autor, estrategias tales como la difusión de propaganda o la desinformación para desmoralizar o manipular al enemigo y al público son propias en esta instancia y sobre la base de ello efectúa la siguiente analogía:

- "Acceder, interrumpir..." El sitio del Poder Judicial fue pasible de un ataque de denegación de servicio (DoS). Este provocó una saturación de demanda de peticiones en un servidor, impidiendo su resolución oportuna y el consecuente colapso. Por eso se le denomina *denegación*, pues hace que el servidor no pueda atender a la cantidad enorme de solicitudes
- "Destruir, alterar..." Algunas fuentes del poder judicial, alegaron que "se perdieron expedientes..." Habrá que demostrarlo, sin embargo, desnuda la situación de una errónea manera de administrar los planes de contingencia y, como quedó dicho, no se clasificaron activos ni se tomaron periódicas copias de resguardo de la información sensible.
- Operaciones de Información: Quedó demostrado que, ante el ataque, la publicidad sobre "una nueva manera de manejarse en Tribunales y Comodoro Py" es al menos, falaz. Nadie confiará su suerte a los ya denostados y/o dudosos juicios de los actores intervinientes en el procesamiento, sentencia o condena de una persona.
- Operaciones Psicológicas: Queda para la "grey y la plebe" si semejante entidad de administración de justicia padece los malestares de un grupo que desafía al poder en su totalidad, demostrando coraje o incordura (esta última de carácter de inimputabilidad), anonimato y capacidad por sobre uno de los poderes del Estado. El que debiendo estar ciego, pareciera que tiene el poder de la premonición para descubrir, del jardín de los senderos que se bifurcan, cuál es el más conveniente. ¿Confiarían los "testigos protegidos" en tamaño escándalo y mala prensa, si la protección a la cual se someten, se encuentran al alcance de terceros?

El 31 de enero de 2017, el portal Infobae publicaba[472]:

> Hackearon más de 30 correos oficiales del Ministerio de Seguridad. Lo confirmó una pericia de la Policía Federal. Entre las cuentas afectadas está la de Patri-

471 Barbeito, Gabriel, La Ciberdefensa, Universidad de Belgrano, Centro de Estudios para la Defensa Nacional, Boletín N° 22, noviembre de 2016.

472 Angulo, Martín, Hackearon más de 30 correos oficiales del Ministerio de Seguridad, Disponible en: http://www.infobae.com/politica/2017/01/31/hackearon-mas-de-30-correos-oficiales-del-ministerio-de-seguridad/

cia Bullrich, a quien le intrusaron la cuenta de Twitter. El trabajo también determinó que todo comenzó con un mail falso de la embajada de Bolivia mediante el *"phishing"*, uno de los engaños cibernéticos más conocidos para poder obtener la contraseña de un mail o del banco de una persona.

Quienes así actuaron: ¿a qué otros lugares tuvieron acceso?, ¿qué otras informaciones modificaron, interrumpieron, alteraron o distribuyeron?

Si bien Rusia y China también consideran en su doctrina las operaciones de información, las mismas difieren en algunos aspectos respecto de las de los países de la OTAN.

Para el embajador David J. Smith[473],

> Rusia tiene un concepto más amplio de la guerra de la información, que incluye inteligencia, contrainteligencia, engaño, desinformación, guerra electrónica, debilitamiento de las comunicaciones, degradación de las ayudas a la navegación, presión psicológica, degradación de los sistemas de información y propaganda. Las computadoras son sólo algunas de las muchas herramientas de guerra de la información, que trabajan 24 horas al día, siete días a la semana, en guerra y en paz. Visto de esta manera, los ataques de denegación de servicio distribuido (DDoS), el ciberespionaje y el programa de televisión Russia Today son todas las herramientas relacionadas con la guerra de la información.

En concordancia con esta opinión, Jolanta Darczewska[474] sostiene que "*Los términos 'guerra cibernética' 'guerra de la información' y 'guerra de red de computadoras' tienen significados completamente diferentes en Rusia*".

La mayoría de los autores rusos, explica Darczewska,

> ...entienden la 'guerra de la información' como una forma de influir en la conciencia de las masas como parte de la rivalidad entre los diferentes sistemas de civilización adoptados por diferentes países en el espacio de la información mediante el uso de medios especiales para controlar los recursos de la información como 'armas de información'. Ellos así mezclan el orden militar y no militar y la tecnológica (espacio cibernético) y el orden social (espacio de información) por definición y hacen referencias directas a la 'Guerra fría' y 'guerra psicológica' entre el este y el oeste.

Para Gurmeet Kanwal[475] tampoco "hay ninguna ambigüedad en la manera en que

---

473 Smith, David J. Russian Cyber Capabilities, Policy and Practice; Focus Quarterly, Winter 2014; The Jewisw Policy Center; Disponible en: http://www.jewishpolicycenter.org/2013/12/31/russian-cyber-capabilities/

474 Darczewska, Jolanta; The Anatomy of Russian Information Warfare: The Crimean Operation, a case Study; Centre for Eastern Studies, May 2014; Disponible en: http://www.osw.waw.pl/sites/default/files/the_anatomy_of_russian_information_warfare.pdf.

475 Gurmeet, Kanwal; China's Emerging Cyber War Doctrine; Journal of Defence Studies; Vol 3. No 3. July 2009; Disponible en: http://idsa.in/system/files/jds_3_3_gkanwal_0.pdf.

los chinos consideran a las operaciones de información". Para ellos, según el autor, estas comprenden:

- Las operaciones de inteligencia que incluyen reconocimiento de inteligencia y protección.
- Operaciones de mando y control para interrumpir el flujo de la información enemiga y debilitar su capacidad C^2 mientras se protege la propia.
- Guerra electrónica asumiendo la iniciativa electromagnética a través del ataque electrónico, la protección electrónica y el apoyo de guerra electrónica.
- Ataque a las redes y sistemas informáticos enemigos para dañar y destruir computadoras críticas, las redes y los datos almacenados en ellas.
- Destrucción física de las fuentes enemigas tales como la infraestructura de la información como C4ISR.

Para el experto Larry Wortzel[476],

Los conceptos operacionales del Ejército de Liberación Nacional para el empleo tradicional de las señales de inteligencia y guerra electrónica se han expandido para incluir la guerra cibernética; cinética y ciberataques a satélites; y las operaciones de confrontación de la información a través del espectro electromagnético. Los militares chinos, sin embargo, tienen la aparente intención de llevar a cabo estas actividades en los niveles táctico, operacionales y estratégicos de la guerra, imaginando atacar la infraestructura crítica y los puntos de embarque de la nación enemiga. Junto con estos aspectos más técnicos de las operaciones de información, la combinación de la guerra psicológica; la manipulación de la opinión pública, o guerra de los medios de comunicación; y la manipulación de los argumentos jurídicos para fortalecer la posición diplomática y de seguridad china, o lo que China llama "guerra legal", se unen en una perfeccionada doctrina de operaciones de información.

Como puede apreciarse, las operaciones de información a las que pueden contribuir las operaciones cibernéticas, no deben entenderse como algo exclusivo de occidente. Si bien están explicadas en la mayoría de las doctrinas de los países occidentales, también las llevan a cabo países como Rusia y China y, como se verá, en estos países, estas operaciones están mucho más integradas con las operaciones cibernéticas y la guerra electrónica que en occidente.

Las operaciones de información no están catalogadas en la República Argentina. Como el modelo de la administración gubernamental durante el período 2003/2013 implementó la absoluta veda de los militares en el marco interno, y se restringió el accionar militar al "enemigo militar estatal externo", de conformidad con ello se prohibieron las operaciones de información dado que el supuesto básico era que ningún país iba a atacar a la Argentina.

---

476 Wortzel, Larry M.; The Chinese People's Liberation Army and Information Warfare; U.S. Army War College, Strategic Studies Institute; Marzo 2014; Disponible en: http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA596797

Bien puede decirse que esta es una concepción ideológica obsoleta basada en la Escuela de Frankfurt y la aplicación del pensamiento único al socialismo en el marco del materialismo histórico, concepción de Relaciones Internacionales que fracasó al descubrirse en sus seguidores enormes campañas de corrupción.

Antecedentes

A partir de la caída del Muro de Berlín se produjo un cambio en el paradigma de la seguridad internacional debido a que, de una segura confrontación entre las superpotencias, se comenzaron a percibir otras interacciones más complejas entre actores estatales y no estatales. La globalización, la competencia por los recursos naturales y las tensiones en las estructuras políticas y sociales se combinaron con distintas ideologías, religiones y culturas que aumentaron la incertidumbre. También se generaron expectativas en algunas sociedades occidentales[477], reforzadas por la exposición de los medios de comunicación especializados en temas de relaciones internacionales, respecto de que el conflicto y la confrontación quedarían limitados por códigos morales cada vez más regulados por las progresivas y más extensas obligaciones legales.

Al mismo tiempo, se originó una revolución de la información (especialmente con el avance de Internet y las nuevas aplicaciones de los teléfonos móviles) que se inició en una época de toma de decisiones basadas en computadoras. Esta evolución de la información consta de información, actores y sistemas que permiten el uso de la información. Los actores son líderes mundiales, decisores, individuos y organizaciones. La información también incluye los materiales y sistemas empleados para recopilar, aplicar o difundir dicha información. El ambiente de la información propiamente dicho es donde los seres humanos y sistemas automatizados observan, orientan, deciden y actúan, y por lo tanto es el principal ambiente de toma de decisiones.

La opinión pública que en la primera mitad del siglo XX no tenía mayor importancia, en la segunda mitad de ese mismo siglo pasó a condicionar hasta la política exterior de los estados. Francia en Argelia, y Estados Unidos en Vietnam habían triunfado militarmente, pero perdieron la guerra por presiones de la opinión pública. En los comienzos del siglo XXI, simultáneamente, redes sociales como *Facebook, Twitter, Linkedin o Instagram* cuyo propósito era relacionar a individuos u organizaciones de acuerdo a algún criterio (relación profesional, amistad, parentesco, etc.) fueron desarrollándose. No puede soslayarse que durante los primeros días de la "Primavera Árabe" de 2011 las dos primeras constituyeron una muestra clara de cómo pueden quedar abrumados aquellos gobiernos que deben lidiar con una opinión pública que decide manifestarse, valga la redundancia, públicamente, y que para hacerlo se auto convoca de manera muy rápida a través de dichas redes sociales.

---

477 Basta recordar a Francis Fukuyama, conocido por haber escrito, en 1992, el libro "El fin de la Historia y el último hombre" en el que defiende la teoría de que la historia humana como lucha entre ideologías ha concluido y ha dado inicio a un mundo basado en la política y economía de libre mercado que se ha impuesto a lo que el autor denomina utopías tras el fin de la Guerra Fría.

En la actualidad, millones de personas y empresas efectúan llamadas y video llamados a través de software denominados *Skype o WhatsApp*, que permiten que "todo el mundo" se comunique entre sí.

También, hoy en día, el empleo de plataformas multicanal y redes sociales como las mencionadas *Facebook, Twitter, Instagram, Flickr o Youtube* permite a cualquier actor recopilar una enorme cantidad de información sobre sus potenciales adversarios e influir en la opinión pública mediante actividades de propaganda y contra-propaganda[478] como también, tal cual lo hace el Hamás, realizar un barrido continuo de las principales redes sociales en busca de perfiles de soldados de las Fuerzas de Defensa de Israel[479,480]. Es así que "*las fuerzas armadas de muchos países también se han subido al carro de las redes sociales, especialmente para utilizarlas como herramienta de inteligencia y comunicación estratégica*"[481].

Así como el empleo de las redes sociales en el ámbito militar se ha convertido en una importante herramienta de inteligencia y comunicación estratégica, también se ha transformado en una amenaza para la seguridad de las operaciones y un peligro para sus componentes. Es muy notable el caso del Almirante Stavridis, ex Comandante de las Fuerzas Armadas en Europa (SACEUR). En 2012, la imagen y el nombre del Almirante se utilizaron para crear una cuenta falsa de Facebook.

> En poco tiempo, numerosos altos mandos de la OTAN accedieron a la cuenta y compartieron sus datos con su superior y "amigo". Una acción tan simple como esa permitió una recopilación de inteligencia que no solo resultaba gratuita, sino que era proporcionada "gratuitamente" por las propias víctimas[482].

Para hacer frente a la cambiante situación de la seguridad mundial y la aparición del nuevo entorno de la información es que los países comenzaron a desarrollar conceptos, procedimientos y doctrinas que derivaron, entre otras cosas, en que se incorporaran a las operaciones cibernéticas dentro de las "Operaciones de Información", término que se refiere a una serie de diferentes actividades vinculadas entre sí, algunas relacionadas con el flujo de la información y otras con su contenido.

Esa mezcla de lo humano y lo automatizado, para la doctrina militar de los Estados Unidos, de Brasil, de España, de Francia y de otros países no sólo comprende a las operaciones cibernéticas, sino que también abarca a la guerra electrónica, al engaño militar, a

---

478 Fojón Chamorro Enrique y Colom Piella Guillem, "Las redes sociales y sus riesgos para las Fuerzas Armadas"; artículo del Diario El Mundo, España, 22 octubre 2014. Disponible en: http://www.elmundo.es/tecnologia/2014/10/22/5447427cca474150258b456c.html

479 Fojón Chamorro Enrique, "El Estado Islámico y la guerra cibernética", Blog del Real Instituto Elcano, 20 abril 2015. Disponible en: http://www.blog.rielcano.org/estado-islamico y-guerra cibernética/

480 Según estimación de las propias FDI, el 70% de sus generales, oficiales y suboficiales y el 95% de sus soldados disponen de perfil personal en Facebook.

481 Singer P. W. & Friedman A; Cybersecurity and Cyberwar What Everyone Needs to Know; Op. Cit.

482 Gómez de Ágreda, Ángel "Integrando lo "Ciber" en las Operaciones"; Revista de Aeronáutica y Astronáutica; N° 846; P. 720; 2015; Disponible en: http://publicaciones.defensa.gob.es/pprevistas/be4ba46b-fb63-65ab-9bdd-ff0000451707/index.html#/18/

las operaciones de seguridad y a las operaciones de apoyo a la información (ex operaciones psicológicas), al ataque físico y al ataque por red informática[483].

Para Guillem Colom[484],

> En Israel, Líbano, Palestina, Siria, Ucrania, Crimea o el Estado Islámico, se han empleado plataformas multicanal y redes sociales como Facebook, Twitter, Instagram, Flickr o Youtube para recopilar un vasto volumen de información sobre su enemigo susceptible de transformarse en inteligencia útil para las operaciones y también influir en la opinión pública propia, adversaria y neutral mediante actividades de propaganda y contra-propaganda. Precisamente por ello, muchos ejércitos han integrado la dimensión cibernética en las labores de comunicación estratégica; realizan operaciones de información (INFOOPS) y operaciones psicológicas (PSYOPS) en el ciberespacio; llevan a cabo actividades de inteligencia de fuentes abiertas (OSINT) en Internet e incluso explotan la valiosa información que proporcionan las redes sociales virtuales (SOCMINT).

Para Stel, el objetivo de las operaciones de información es "dañar, destruir o modificar la información contenida en las redes y sistemas para generar un cambio en lo que la población piensa o conoce"[485].

Un ejemplo de ello lo muestran Fojón Chamorro y otros autores[486] para quienes,

> Tras perder la "batalla de las narraciones" en los conflictos del Líbano (2006) y Gaza (2008-09), las Fuerzas de Defensa de Israel (FDI) se vieron obligadas a replantear sus métodos y herramientas de comunicación estratégica. En la operación "Pilar Defensivo" de noviembre de 2012 Israel explotó el potencial de los medios de comunicación digitales – especialmente las redes sociales, las plataformas multimedia y los blogs– para informar de sus acciones y alterar la percepción pública del conflicto.

Si bien las denominadas operaciones de información se han venido desarrollando desde la Primera Guerra del Golfo, dada la relación existente entre las redes sociales y el espacio cibernético, el concepto como tal fue variando en el tiempo debi-

---

483 Joint Publication 3-13. Op. Cit

484 Colom Piella, Guillem, Director de THIBER, the cybersecurity Think Tank, Ciber Elcano, Informe mensual de ciberseguridad, diciembre 2016, Nº 20 P 11. Disponile en: http://www.realinstitutoelcano.org/wps/portal/rielcano_es/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_es/zonas_es/ciber-elcano-20-diciembre-2016

485 Stel, Enrique; "Guerra Cibernética" Ed. Círculo Militar, Ira. Edición, Ed 2005, Buenos Aires, Argentina P. 54

486 Fojón Chamorro, Enrique, Hernández Llorente, Adolfo y Colom Piella, Guillem; "Las redes sociales como herramienta de comunicación estratégica de las Fuerzas de Defensa de Israel durante la operación Pilar Defensivo en Gaza"; Real Instituto Elcano; ARI 94/2012 Disponible en: http://www.realinstitutoelcano.org/wps/portal/rielcano/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_es/zonas_es/ari94-2012_fojon-hernandez-colom_redes_sociales_israel_pilar_defensivo

do a que, desde aquel entonces, el espacio cibernético fue utilizado como lo fue en Georgia en 2008, donde las operaciones cibernéticas se ejecutaron para alterar las capacidades de la nación en paralelo con una ofensiva terrestre o, como ocurrió en Siria, donde los medios cibernéticos fueron empleados para apoyar el régimen de Assad y sus políticas.

En 2006, para el Estado Mayor Conjunto de los Estados Unidos,[487] las operaciones de información se componían de cinco capacidades principales: operaciones psicológicas, engaño militar, operaciones de seguridad, guerra electrónica y operaciones de redes de computadoras. Según la publicación, de las cinco, las tres primeras habían jugado una parte importante en las operaciones militares durante muchos siglos, pero en esta era moderna se han ido incorporando primero las de guerra electrónica y más recientemente las de redes de computadoras.

En la más reciente edición de 2014[488] las operaciones de información son,

> ...caracterizadas como el empleo integrado, durante las operaciones militares, de las capacidades relacionadas con la información[489] (IRCs) en concierto con otras líneas de operación para influir, alterar, corromper o usurpar la toma de decisiones de adversarios y potenciales adversarios al mismo tiempo que se protegen las propias.

En la República de Ecuador, en julio de 2014, el Jefe del Comando Conjunto de las Fuerzas Armadas promulgó el "Manual de Operaciones de Información[490]" en el cual,

> ...en el capítulo I se considera el ámbito de la información y su relación con las operaciones militares. En el capítulo II se analizan las capacidades principales de las Operaciones de Información necesarias para planificar y ejecutar con éxito las Operaciones de Información, incluyendo las capacidades principales, las capacidades de apoyo y las capacidades relacionadas en un ambiente conjunto. El capítulo III trata del apoyo de la Inteligencia a las Operaciones de Información, revelando la importancia de las labores de esta especialidad para la preparación, planificación y evaluación de las Operaciones de Información. El capítulo IV designa las responsabilidades y las relaciones de mando en las Operaciones de Información. El capítulo V analiza la planificación y coordinación de las Operaciones de Información. En el capítulo VI se aborda la educación militar en la planificación, ejecución, evaluación y control de las Operaciones de Información.

---

487 Joint Publication 3-13. Op. Cit.

488 Ibídem

489 IRCs (Information Related Capabilities) son las herramientas, técnicas o actividades que afectan las tres dimensiones del ambiente de la información: la física, la informativa y la cognitiva.

490 Slide Share Fuerzas Armadas del Ecuador. Comando Conjunto. Disponible en: http://es.slideshare.net/kaluco/manual-de-operaciones-de-informacin-resolucin-14-diedmild003-del-14-de-agosto-de-2014

Dicho manual ecuatoriano describe a las Operaciones de Información como:

...el empleo integrado de las capacidades principales y de apoyo que se desarrollan en los procesos de Operaciones de Información aplicables a las amenazas propias con lo que es coherente con los procesos de restructuración de las Fuerzas Armadas, y que se detallan a continuación: 1. Capacidades Principales: - Operaciones Psicológicas - Operaciones de Decepción y Engaño - Telecomunicaciones y Guerra Electrónica - Seguridad en las Operaciones (Ciberseguridad) 2. Capacidades de Apoyo: - Inteligencia para Operaciones de Información 3. Capacidades Relacionadas: - Comunicación social.

Según, Jolanta Darczewska[491]

> La guerra de la información se trata de una especie de batalla entre partes que se lleva a cabo por medios convencionales y no convencionales, abiertos y secretos, mediante estructuras organizativas tanto militares como no militares (fuerzas especiales, fuerzas armadas irregulares, oposición interna en el país enemigo). En el pensamiento y en la doctrina militar rusa, la guerra de la información tiene dos dimensiones: una amplia (como una clase de combate librado en forma separada en todos los niveles: políticos, económicos, diplomáticos, humanitarios, militares) y otra más estrecha (como un elemento de apoyo para la acción militar).

Darczewska también señala que,

> ...en la doctrina rusa, no se encuentra ninguna idea con respecto a la 'cibernitetización' de los conflictos armados, o cualquier mención sobre herramientas electrónicas para la 'ciberguerra', es decir, la destrucción de recursos de información del enemigo la cual– como podríamos pensar – debería ser una responsabilidad de las fuerzas armadas y por lo tanto verse reflejada en el documento que estamos analizando". No encontramos en él ninguna definición precisa de 'espacio de información', 'guerra de la información', 'operaciones asimétricas', 'medios no militares de la guerra', 'contención no nuclear' u otros términos relacionados. Al mismo tiempo, dichos términos aparecen como parte de las ideas en circulación en Rusia, que se presentan como una respuesta rusa a la llamada por occidente 'guerra híbrida' (contra Ucrania, Rusia y otros países), lanzada con el objetivo de bloquear la estrategia de integración de los Estados postsoviéticos con la Unión Europea y la OTAN.

Sin embargo, según José Miguel Palacios[492], *"para el Jefe del Estado Mayor General ruso General Valeri Gerasimov la "guerra informativa" es sumamente importante en lo*

491 Darczewska, Jolanta, "The devil is in the details: Information Warfare in the light of Russia's Military Doctrine, Point of View, Number 50, Warsaw, May 2015, Disponible en: https://www.osw.waw.pl/sites/default/files/pw_50_ang_the-devil-is-in_net.pdf

492 Palacios, José Miguel, "La doctrina Gerasimov: segunda entrega", 11 de abril de 2016, Análisis GESI, 7/2016. Disponible en: http://www.seguridadinternacional.es/?q=es/print/802

que él denomina la "guerra híbrida"[493] *pues sus efectos son comparables a los del uso masivo de tropas".*

Para Gerasimov,

> Hay que prestar una atención especial al que es el elemento esencial de los métodos híbridos. La falsificación de los acontecimientos y la limitación de la actividad de los medios de información se convierten en uno de los métodos asimétricos más eficaces para la conducción de las guerras. Su efecto puede ser comparable a los resultados de un uso masivo de tropas.

En un artículo muy referenciado sobre la guerra moderna, publicado en Military Review, el General Valery Gerasimov[494] argumentó *"que los medios no militares se utilizan cuatro veces más a menudo en los conflictos modernos que las medidas militares convencionales".*

Para Christopher S. Chivvis[495]

> Capturar el territorio sin tener que recurrir a la fuerza militar abierta o convencional fue el objetivo de la exitosa anexión de Crimea a Rusia en el año 2014, una jugada que puso en marcha el debate sobre las "estrategias híbridas" rusas. La anexión de Crimea se basó en gran medida en el empleo sobre todo de fuerzas especiales que operaron a través de un comando de operaciones especiales ruso recién creado. El uso de estas tropas de élite, junto con una campaña de guerra de la información y el despliegue de grupos que tienen una amplia simpatía con los objetivos de Rusia (proxies), creó las circunstancias que sentaron las bases para una adquisición convencional, sin derramamiento de sangre, de Crimea. Rusia había utilizado previamente algunas tácticas en su invasión a Georgia en 2008. Los conflictos en Ucrania y Georgia quedaron "congelados" obstaculizando los esfuerzos de estos países hacia la integración con Europa occidental.

Consecuentemente, surgen determinados interrogantes tales como: ¿qué es el ambiente de la información?; ¿cuál es la relación entre las operaciones de información y las

---

493 Palacios, Gerasimov utiliza el concepto "guerra híbrida" o sus derivados en un sentido distinto del que es habitual en Occidente. Hoffman, el padre del concepto, la "guerra híbrida incorpora toda una serie de diferentes formas de hacer la guerra, incluyendo medios convencionales, tácticas y formaciones irregulares, atentados terroristas, incluyendo violencia y coerción indiscriminadas, y desorden criminal" (Hoffman, 2007:14). Es decir, en la guerra híbrida se combinan acciones militares convencionales con otras propias de la guerra irregular. Como explicaba el coronel español Calvo Albero en 2009, en la "guerra híbrida" "al menos uno de los adversarios recurre a una combinación de operaciones convencionales y guerra irregular, mezclada esta última con acciones terroristas y conexiones con el crimen organizado" (Calvo, 2009:11). En cambio, para Gerasimov, "métodos híbridos" son, precisamente, los que van más allá de los métodos militares tradicionales.

494 Gerasimov, Valery The Value of Science is in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations, Military Review, January-February 2016. P. En 2016, el autor era General del Ejército y Jefe del Estado Mayor de las Fuerzas Armadas de la Federación Rusa.

495 Chivvis, Christopher S. Testimony of The RAND Corporation Understanding Russian "Hybrid Warfare" and What Can be Done About It. Disponible en: http://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT468/RAND_CT468.pdf

operaciones cibernéticas?; ¿cuál es la diferencia entre operaciones de información, operaciones cibernéticas y las operaciones de red de computadoras?; ¿cómo se incorporan las operaciones de información en el planeamiento operacional?

Por tal motivo, en este capítulo se tratarán las operaciones cibernéticas y las operaciones de información y su relación con el ambiente de la información, mostrando su interrelación y su empleo en los conflictos más recientes, en virtud de que, como se verá, las operaciones cibernéticas proporcionan una capacidad de acceso a redes digitales para interrumpir, negar, degradar o destruir su capacidad, o bien para interceptarlas y utilizarlas como un mecanismo de las operaciones psicológicas y de operaciones de engaño, lo que podría llegar a afectar la voluntad de un actor, su capacidad o entendimiento en función de la dependencia de ese actor de tales redes. Hacia el final, se concluirá con una propuesta de incorporación de dichas operaciones dentro del planeamiento de una campaña.

El ambiente de la información

Al igual que ocurría durante la Guerra Fría cuando desde aviones se distribuían panfletos a quienes vivían detrás de la "Cortina de Hierro" con la finalidad de que dispusieran de otro tipo de información que el estado soviético les ocultaba, en la actualidad, a través de Internet es posible no solo difundir dicha clase de información, sino también permitir que los ciudadanos de un país se comuniquen entre ellos y con otras partes del mundo, aun, cuando el estado les haya bloqueado el acceso a las redes sociales[496].

No solo eso. El poder de las redes sociales durante las elecciones en distintos países, en los incidentes callejeros en regímenes represivos o durante desastres naturales, ha demostrado su capacidad de cambiar los medios tradicionales de comunicación, que simplemente transmitían en un solo sentido la información desde una agencia de noticias. Con este cambio en los medios de comunicación, las grandes agencias de noticias también se aprovecharon del material de archivo generado por el usuario y por ello, algunos gobiernos han interferido y limitado el acceso a fuentes de información, sobre todo de las redes sociales que proporcionan información instantánea.

Paralelamente, el desarrollo de dispositivos inteligentes de comunicación permitió que en el mismo día un *smartphone* pueda ser empleado por células terroristas para vincularse a través de Twitter y coordinar un ataque más allá de las fronteras internacionales, y como un medio de detonación de un Dispositivo Explosivo Improvisado (IPD) en una carretera de algún lugar del mundo.

Un video puede tomarse en el mismo *smartphone* inmediatamente después de un ataque bomba y ser fácilmente subido a *YouTube*. En cuestión de minutos, millones de televidentes alrededor del mundo podrán ser capaces de ver los daños causados por la explosión. En contraposición, la Agencia Nacional de Seguridad estadounidense (NSA), ha proporcionado apoyo a sus Fuerzas Armadas durante las guerras de Irak y

496 Ibidem

Afganistán para evitar que las fuerzas insurgentes compartiesen en Internet videos de los atentados perpetrados contra las tropas estadounidenses[497].

El uso de *selfies* tomadas por los combatientes de ISIL[498] en Siria o Irak ha servido a Estados Unidos para identificar su ubicación y a las pocas horas atacarlos por medio de drones dirigidos desde algún lugar de ese país. A su vez, según el centro norteamericano de vigilancia de los sitios islamistas (SITE), un grupo autodenominado "División de Piratas del Estado Islámico" del Estado Islámico (EI) difundió en Internet los supuestos nombres y direcciones de 100 infantes de marina norteamericanos, acompañados de fotografías, e instó a sus partidarios a asesinarlos[499].

Hackers del *Syrian Electronic Army* (SEA) sedujeron a opositores al gobierno del presidente Asad, utilizando mujeres, una de las cuales, tras conversar un rato con ellos les envió, vía Skype, una foto acompañada de un *malware* lo cual les permitió sustraer *"toneladas de documentos internos sobre planes de operaciones militares contra las fuerzas del presidente Asad"*[500] En una operación, el grupo envió mensajes electrónicos a los rebeldes haciéndose pasar por alguien que conocían o que podían llegar a conocer. Estos mensajes alentaban a las víctimas para descargar una tecnología de comunicaciones llamada *Freegate* diseñada, supuestamente, para ayudar a los disidentes a burlar los organismos de vigilancia del estado. El programa era en realidad un *malware* que permitía al intruso monitorear lo que estaba escribiendo en su computadora el usuario infectado y también a leer y eliminar sus archivos. En otras palabras, los hackers pro-Assad utilizaron el miedo de los espías de Assad para iniciar *snooping*[501] entre ellos. En la segunda operación, a las víctimas les fueron enviados mensajes animándoles a hacer clic en un enlace con un sermón dado por un clérigo partidario de la oposición. Cuando lo hicieron, activaron un programa que colocaba al equipo del usuario bajo el control de los hackers[502].

Todo ello es posible debido a que el espacio cibernético, que es una creación humana, permite que el mundo interactúe, intercambie información, conduzca negocios, etc. Durante siglos, los espías sólo podían escuchar las comunicaciones enemigas. En la actualidad una vez *hackeada* una computadora, como se ha podido apreciar, no sólo se puede leer, cambiar y descargar su contenido, sino también interrumpirlo, corromperlo o borrarlo y engañar o desorientar a quienes lo utilizan. Ello hace que el uso del espacio cibernético resulte sumamente interesante y, en algunos casos, único en la guerra debido al impacto directo e inmediato que puede tener sobre el campo de batalla.

---

497 Blog Tecnológico Ticbeat, De Estonia a Ucrania, la evolución de los conflictos en el espacio cibernético; 28 marzo 2014, Disponible en: http://www.ticbeat.com/seguridad/de-estonia-ucrania-la-evolucion-de-los-conflictos-en-el-espacio cibernético/.

498 ISIL: Islamic State of Iraq and the Levant

499 Diario La Nación, Otra amenaza de El filtran sus hackers datos de 100 marines, 23 marzo 2015. Disponible en: http://www.lanacion.com.ar/1778425-otra-amenaza-de-ei-filtran-sus-hackers-datos-de-100-marines.

500 Yahoo! noticias, AFP 2 febrero 2015, Por una bella mujer en Skype los rebeldes sirios se dejan piratear, Disponible en: https://es-us.noticias.yahoo.com/bella-mujer-skype-rebeldes-sirios-dejan-piratear-182708097.html.

501 Husmear en los asuntos privados de los demás.

502 Shane, Harris; "How Did Syria's Hacker Army Suddenly Get So Good?" Disponible en: http://foreignpolicy.com/2013/09/04/how-did-syrias-hacker-army-suddenly-get-so-good/.

Así como desde la antigüedad los militares de todo el mundo desarrollaron operaciones de engaño para tratar de ingresar en las mentes del oponente y de influir en sus procesos de toma de decisión, en la actualidad, la idea es utilizar la moderna tecnología para alcanzar los mismos fines. El objetivo podrá variar desde uno de nivel estratégico militar, como podría ser impartir órdenes falsas desde un alto mando militar, hasta otro de nivel táctico, tal cual lo hicieron las fuerzas israelíes en la Operación Orchard, en 2007, cuando anularon los sistemas de defensa aérea sirios, durante el ataque aéreo a la planta de procesamiento de plutonio en *Kibar*, pero el efecto es el mismo.

Para[503] Singer y Friedman,

> El éxito de uno de estos ataques podría ser un factor multiplicador debido al impacto que podría llegar a producir en las mentes de los usuarios de las redes bajo ataque. Sólo un porcentaje relativamente pequeño de los ataques tendría que ser exitoso para plantar semillas de duda en cualquier información proveniente de una computadora. Dichas dudas llevarían a los usuarios a cuestionar y comprobar todo, desde sus órdenes hasta las direcciones. El impacto podría ir más allá de la simple interrupción de un sistema de armas, podría erosionar la confianza en todas las redes militares, necesarias para poder operar de manera eficaz.

Hoy en día, tanto las personas, los gobiernos como los ejércitos modernos dependen en gran medida de las TIC y del espacio cibernético especialmente. Por su parte, los medios de comunicación son una herramienta importante que enmarcan la opinión y el estado psicológico de ánimo de la población. Se encuentran ampliamente interrelacionados a través de redes que no sólo permiten que la información se difunda fácilmente, sino que son susceptibles de ser secuestradas para empañar la imagen de los políticos y el gobierno de una nación o para infundir miedo y caos entre la gente.

Las redes sociales, *Facebook, Google+, Hi5, Linkedin, Microbloggin, Twitter,* para citar solo las más conocidas, podrán no ser aptas para reunir gente que construya las nuevas instituciones de un Estado, pero sí para organizar manifestaciones capaces de derrocar gobiernos.

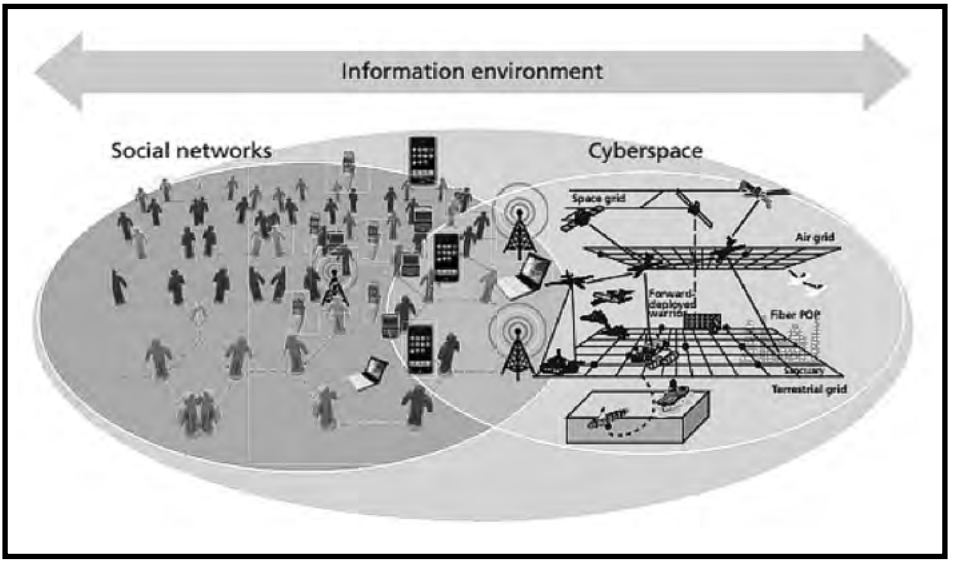
Es por ello que resulta conveniente pensar en el ambiente de la información como dos áreas que parcialmente se interceptan: las redes sociales y el espacio cibernético, tal como se muestra en la figura 9. Las redes sociales son las redes de interacción y relación entre los individuos que continúan creciendo en tamaño, importancia e influencia, afectando no sólo cómo comunicarnos unos con otros, sino también cómo encontrar empleo, vivienda y hasta las relaciones sentimentales; pero las redes sociales también influyen en la evolución del conflicto moderno, pues pueden ser explotadas para manipular la opinión y la percepción de los individuos y, dada la capacidad de permanecer indetectados, les permite a determinados actores utilizar los medios sociales de comunicación que tienen un alcance global para organizar, planificar y realizar distintos tipos de operaciones militares.

---

503 Singer, P. W. & Friedman, Allan; "Cybersecurity and Cyberwar What Everyone needs to know". Oxford University Press; Ed. 2014; P. 127

El ciberespacio, por su parte, es un dominio global dentro del entorno de información de la red interdependiente de las infraestructuras de tecnología de información y los datos de residentes, que incluye la Internet, las redes de telecomunicaciones, sistemas informáticos y procesadores embebidos y controladores[504].

FIGURA 9[505]: EL AMBIENTE DE LA INFORMACIÓN INCLUYE LAS REDES SOCIALES Y EL ESPACIO CIBERNÉTICO[506]



Desde un punto de vista más específico, puede decirse que el ambiente de la información es el conjunto de individuos, organizaciones y sistemas que recogen, procesan, difunden o actúan sobre la información y que se puede desglosar en las dimensiones física, informativa y cognitiva.

La dimensión física se compone de los sistemas de comando y control (C^2), quienes toman las decisiones y la infraestructura de apoyo que permite a los individuos y or-

504 Joint Publication JP 3-12 (R); Cyberspace Operations; 5 February 2013; P. I-2 Disponible en http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf.P. II-9

505 Porche, Isaac R. III, Christopher, Paul, York, Michael Chad C. Serena, Jerry M. Sollinger, Elliot Axelband, Endy M. Daehner, and Bruce J. Held, Redefining Information Warfare Boundaries for an Army in a Wireless World, Santa Monica, Calif.: RAND Corporation, MG-1113-A, 2013. Disponible en: http://www.rand.org/pubs/monographs/MG1113.html.

506 Poole, Matthew & Schuette, Jason. "Cyber Electronic Warfare." Marine Corps Gazette. Disponible en: https://www.mca-marines.org/gazette/2015/08/cyber-electronic-warfare Aunque no se muestra en la figura, las áreas definidas doctrinariamente, como guerra electrónica, Operaciones de redes de computadoras, operaciones psicológicas y operaciones en el ambiente electromagnético, también deben ser incluidas. El ambiente de información, es el conjunto de individuos, organizaciones o sistemas que coleccionan, procesan o diseminan información; también incluye a la información propiamente dicha.

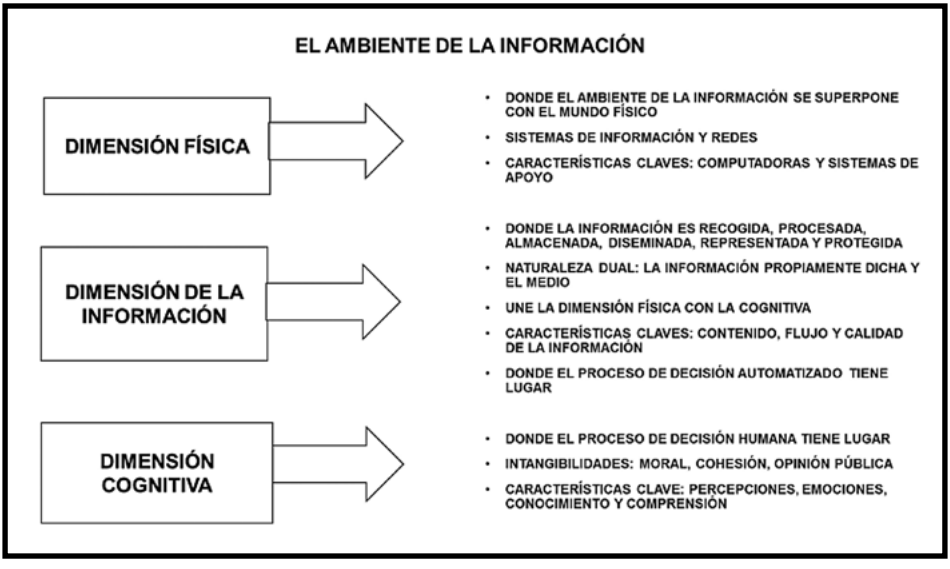
ganizaciones llevar a cabo las operaciones. Es la dimensión en la que se encuentran las plataformas físicas y las redes de comunicación que las conectan. La dimensión física incluye, pero no se limita a los seres humanos, instalaciones C^2, periódicos, libros, torres de microondas, computadoras, notebooks, teléfonos inteligentes, *tablets* o cualquier otro objeto que esté sujeto a la medición empírica.

La dimensión informativa es el lugar donde la información es recogida, procesada, almacenada, diseminada y protegida. Es la dimensión donde se ejercita el C^2 de las fuerzas militares modernas y donde se transmite la intención del comandante. Acciones en esta dimensión afectan el contenido y el flujo de información.

Este dominio informativo tiene influencia en lo que se denomina la preparación de inteligencia en el campo de batalla desde el descifrado de códigos, hasta los reabastecimientos, los movimientos, y la logística. Una vez dentro del sistema de informática y telecomunicaciones de un adversario, se podría desde interrumpir o anular el sistema de comando, la impartición de órdenes, la comunicación entre unidades, afectar los sistemas de armas interconectados para su correcto funcionamiento y/o alterar o anular los sistemas de control de las armas denominadas inteligentes.

La dimensión cognitiva abarca las mentes de aquellos que deben transmitir, recibir y responder o actuar sobre la información. En esta dimensión se piensa, percibe, visualiza, comprende y decide.

FIGURA 10: EL AMBIENTE DE LA INFORMACIÓN[507]



507 FANDOM, Powered by wikia. El ambiente. Disponible en: http://itlaw.wikia.com/wiki/Information_environment

Es por ello que para Héctor Gómez Arriagada[508] las operaciones de información son aquellas ejecutadas en el dominio físico porque "buscan atacar o defender la infraestructura física asociada al Mando y Control y la toma de decisiones, siendo objetivos típicos las redes de comunicaciones, los sensores, medios de búsqueda y los propios Mandos, entre otras; y que son susceptibles de ser afectados por medios cinéticos tradicionales".

Pero también en el espacio cibernético, "Situado al mismo tiempo en las capas lógicas y físicas que intersecan con actividades en, por y sobre el espectro electromagnético, cruzando otros dominios, así como fronteras geográficas y políticas reconocidas". En consecuencia, esto implica una unión entre los dominios tradicionales de la guerra y el espacio cibernético[509].

Y en el dominio cognitivo pues "están destinadas a afectar la percepción por parte de los tomadores de decisiones, siendo el instrumento típico para ello las operaciones psicológicas, aunque también pueden considerarse como parte de las mismas el engaño o la decepción militar".

Concordante con ello, en la última versión de la *Joint Publication 3-12 (R) Cyberspace Operations, el Estado Mayor Conjunto de los Estados Unidos*[510], se observa que:

> ...el espacio cibernético se compone de muchas redes diferentes y a menudo superpuestas, así como los nodos (cualquier dispositivo o ubicación lógica con una dirección de protocolo [IP] Internet u otro identificador análogo) en dichas redes y los datos del sistema (como las tablas de enrutamiento) que los apoyan. Aunque no todas las redes son globalmente conectadas o accesibles, el espacio cibernético continúa siendo cada vez más interconectado. Las redes pueden ser intencionalmente aisladas o subdivididas en enclaves mediante controles de acceso, encriptación, diferentes protocolos o separación física. Con la excepción de la separación física, ninguno puede eliminar la subyacente conectividad física; por el contrario, limitan el acceso.

En ese documento se señala que el espacio cibernético puede ser representado en términos de tres capas: la física, la lógica y la de las ciber-personas, cada una de las cuales representa un nivel en el que pueden llevarse a cabo las operaciones cibernéticas.

La capa física está conformada por el hardware, el software de los sistemas y la infraestructura (cableado, inalámbrico, links, enlaces electromagnéticos, satélites y ópticos) que apoyan la red y los conectores físicos (alambres, cables, radiofrecuencia, *routers*, *switches*, servidores y equipos).

La capa lógica consiste en aquellos elementos de la red que se relacionan uno con el otro de una manera que se abstrae de la red física, por ejemplo, la forma o las relaciones

---

508 Gómez Arriagada, Héctor; "Ciberoperaciones" Disponible en http://www.academia.edu/5087425/Ciberoperaciones.

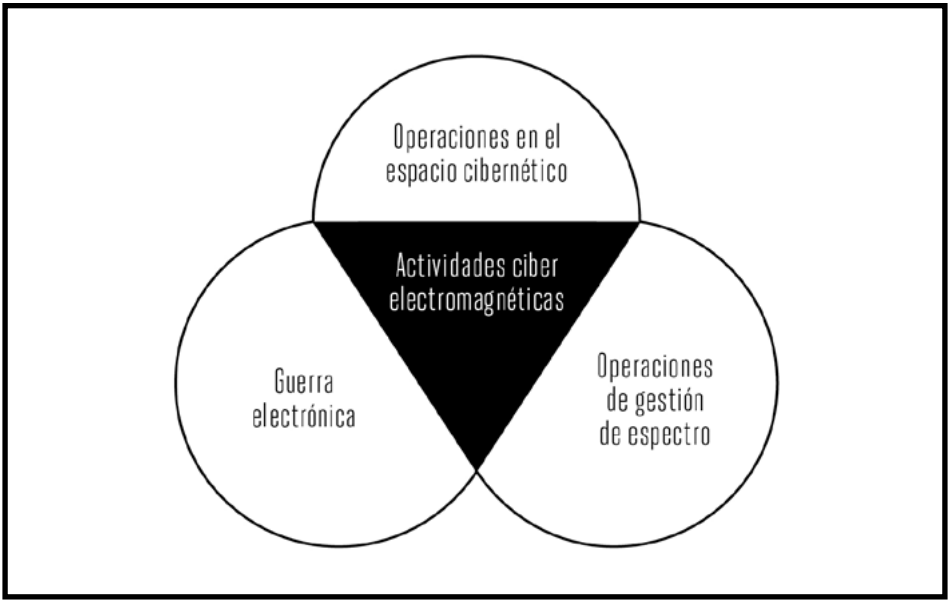
509 Brandes; Sean: The Newest Warfighting Domain: Cyberspace; Synesis: A Journal of Science, Technology, Ethics, and Policy 2013; Potomac Institute Press; Disponible en: http://www.synesisjournal.com/vol4_g/Brandes_2013_G90-95.pdf.

510 Joint Publication JP 3-12 (R); Cyberspace Operations; 5 February 2013; P. I-2 Disponible en http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf.

no están vinculadas a un individuo, ruta de acceso específica o nodo. Un ejemplo simple es cualquier sitio Web que está alojado en los servidores en múltiples ubicaciones físicas donde todo el contenido se puede acceder a través de un único localizador de recursos uniforme[511] (URL).

Por último, la capa de las ciber-personas representa todavía un mayor nivel de abstracción que el de la capa lógica en el espacio cibernético; utiliza las reglas que se aplican en la capa lógica de la red para el desarrollo de una representación digital de un individuo o identidad de la entidad en el espacio cibernético. La capa de las ciber-personas está conformada por las personas que se encuentran realmente en la red. Las ciber-personas pueden referirse directamente a un individuo o entidad, con la incorporación de algunos datos biográficos o corporativos, correo electrónico y direcciones IP, páginas Web, teléfonos, etc. Un individuo puede ser múltiples ciber-personas y una sola ciber-persona puede tener varios usuarios. De allí que la atribución de responsabilidad y la orientación en el espacio cibernético sea difícil de llevar a cabo.

FIGURA 11: ELABORACIÓN PROPIA SOBRE LA BASE DE LAS FUENTES ANALIZADAS[512]



511 El URL Uniform Resource Locator es la cadena de caracteres con la cual se asigna una dirección única a cada uno de los recursos de información disponibles en Internet. Existe un URL único para cada página de cada uno de los documentos de la World Wide Web. El URL de un recurso de información es su dirección en Internet, la cual permite que el navegador la encuentre y la muestre de forma adecuada.

512 Son las funciones interrelacionadas de gestión del espectro, asignación de frecuencias y la política que permite el planeamiento, la gestión y la ejecución de las operaciones dentro del entorno operacional electromagnético.

Este modelo de tres capas se puede utilizar para examinar la propia percepción y representación de la amenaza pues existen tipos especiales de operaciones, de agresores y habilidades específicas que corresponden a cada una de ellas; organizar la ciberdefensa, supone tener en cuenta no solo los aspectos técnicos, sino también las capacidades cognitivas, los aspectos políticos, jurídicos y económicos. Es decir, debe involucrar múltiples habilidades y diferentes sectores (proveedores de servicios de Internet y operadores de telecomunicaciones, proveedores de tecnología, centros de investigación y redes sociales capaces de actuar en el nivel de "manipulación de la información"). Estas consideraciones son las que permiten validar el enfoque holístico de ciberdefensa.

Por otra parte, los elementos del ciberespacio están conectados y apoyados por la infraestructura física, por sistemas electrónicos y por porciones del espectro electromagnético (EMS por su sigla en inglés). En la medida en que se desarrollan nuevas infraestructuras y sistemas, estos usan porciones cada vez más crecientes del EMS, tienen mayor capacidad de procesamiento de datos y velocidad, aprovechan un mayor ancho de banda y hay sistemas que están diseñados para cambiar las frecuencias (los lugares donde operan dentro del EMS) como forma de manipular los datos[513].

Por ello, el Ejército de Estados Unidos (US. Army) ha creado el concepto de Actividades Ciberelectromagnéticas[514] (CEMA), en el que integra las actividades del espacio cibernético con las electromagnéticas debido a que el dominio de actuación de ambas tiene grandes áreas de desempeño que son comunes. Con ello se consigue obtener una sinergia de los efectos de ambos dominios, al tiempo que se coordinan de una forma más eficaz los medios humanos y materiales[515].

El Manual Field M 3-38 *Cyber Electromagnetic Activities,* publicado en febrero de 2014, describe a las CEMA como aquellas actividades que

> ...tienen como objetivo explotar las ventajas sobre el enemigo en el espacio cibernético y en el espectro electromagnético a la vez que, de forma simultánea, le deniega su uso y protege al sistema de mando y control de la misión[516].

A fines de abril de 2016, la General Patricia A. Frost, Segundo Jefe de Operaciones del Ejército de Estados Unidos, expuso que,

> ...recientemente se ha producido un cambio radical en materia de ciberseguridad,

---

513 Introduction to Cyberspace Operations, Op. Cit.

514 Cortés Ruiz, Pedro; El Concepto Doctrinal "Actividades Ciberelectromagnéticas" (CEMA), en el Ejército de Tierra de los Estados Unidos". I Congreso Internacional en Estudios Militares; Granada, del 17 al 19 de septiembre de 2014; Disponible en: http://estudiosmilitares.es/comunicaciones/Pedro%20Cortés%20Ruiz.pdf

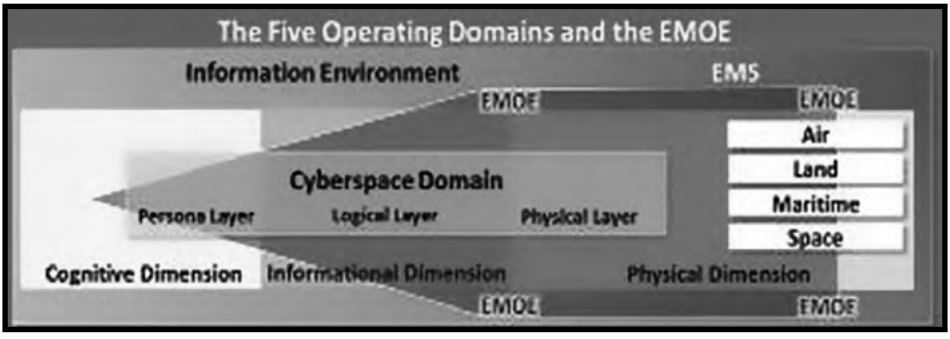
515 Si bien existe una coincidencia en la necesidad de hacer converger las operaciones cibernéticas y las electrónicas, hay también diferencias respecto del entrenamiento, la asignación de recursos, y la organización.

516 US Army, FM 3-38 Cyber Electromagnetic Activities, 2014 Disponible en: https://fas.org/irp/doddir/army/fm3-38.pdf fec.

impactando desde el Cuerpo de Ejército hasta los más bajos niveles"[517]. Este nuevo concepto comprende el desarrollo de capacidades CEMA tanto para protección del territorio nacional como para su empleo durante los despliegues.

Partiendo de que se disponen de las capacidades CEMA, esta concepción permite, entre otras cosas, integrar operaciones aparentemente disímiles entre sí como: establecer, operar y defender una red, atacar y explotar los sistemas del enemigo, tales como sistemas de armas, de mando y control, infraestructuras críticas y recursos clave, adquirir cierto conocimiento de la situación mediante los sistemas inteligentes de combate, *Blue Force Tracking*[518] (BFT), sensores, etc. ,y proteger a los individuos y a las plataformas mediante contramedidas electrónicas, perturbaciones, disminución de interferencias o securización de la información. En síntesis, las CEMA permiten la sincronización de las operaciones en el espacio cibernético, de guerra electrónica y de gestión del espectro, creando efectos combinados que permiten superar las diferencias entre lo ofensivo y lo defensivo.

FIGURA 12: LOS CINCO DOMINIOS OPERACIONALES Y EL AMBIENTE ELECTROMAGNÉTICO OPERACIONAL (EMOE)[519]



Asimismo, el espacio cibernético no existiría sin su componente electrónico y sin el espectro electromagnético (EMS). Las computadoras, los teléfonos inteligentes y el hardware poseen dispositivos electrónicos. El espectro electromagnético da una definición física al espacio cibernético y se relaciona directamente con cómo la información digitalizada se mueve a través de ese espacio. En su forma más simple, la información (palabras, imágenes, archivos, etc.) se convierte en datos digitales en forma de

517 Homesec Grupo Atenea Seguridad Nacional, Disponible en: http://www.homsec.es/las-operaciones-ciberneticas-cema-se-expanden-todos-los-niveles-del-us-army/

518 Significa Seguimiento de fuerzas amigas

519 Poole, Matthew & Schuette, Jason, "Cyber Electronic Warfare." Marine Corps Gazette. Disponible en: https://www.mca-marines.org/gazette/2015/08/cyber-electronic-warfare

código binario electrónico. Los datos digitales, a su vez, se colocan en paquetes y estos se envían vía radiación electromagnética a lo largo de la ruta más segura y rápida entre dos puntos. Así, se envían desde un transmisor a un receptor las señales de radio, televisión, voz y de datos.

Cabe destacar que el grado de integración entre las operaciones cibernéticas, las operaciones de información y las de guerra electrónica varían según las diferentes fuerzas armadas de los Estados Unidos. De hecho, existe una serie de discusiones al respecto de si debiera haber una más profunda integración organizativa y doctrinaria entre los tres tipos de operaciones para facilitar la coordinación de los medios y la eficiencia militar[520].

La globalización de la tecnología de la información ha aumentado la disponibilidad y capacidad de equipos electrónicos multipropósito e incrementado la demanda global de acceso al espectro electromagnético. Del mismo modo, cada vez más dispositivos de comunicación, por ejemplo, celulares, los teléfonos inteligentes, son capaces de transmitir y recibir información de voz y datos, haciendo más difusas las líneas que tradicionalmente separaban los campos de la conducción entre inteligencia, operaciones y comunicaciones.

Esto ha llevado a la integración de las operaciones cibernéticas a la Guerra electrónica, a las operaciones de inteligencia, a las operaciones en el espectro electromagnético y a las operaciones de información.

El empleo de las operaciones de información en los conflictos recientes

Como se ha podido apreciar, las operaciones de información constituyen un vector para la manipulación de las percepciones. Campañas de propaganda y desinformación pueden engañar al oponente e influir en lo que es aceptado como verdadero. Véanse algunos ejemplos de su empleo en los conflictos más recientes.

En 2006, durante el conflicto entre Israel y el Hezbollah, este último hackeó varios sitios web para difundir el mensaje de la televisión satelital Al-Manar (el faro en árabe) a una audiencia global. Específicamente, hackearon una empresa de cable de Texas con el fin de utilizar su dirección de protocolo de Internet (IP) como la base para operar sitios web que transmitiesen la televisión Al-Manar[521].

Cuando en 2008 Rusia invadió a Georgia por tierra y aire y la bloqueó por el mar, simultáneamente los hackers pro rusos anularon la comunicación de Internet de Georgia durante todo el conflicto armado. Previo a la invasión y al bloqueo marítimo, la página web del Presidente georgiano fue el blanco del primer ataque de Denegación de Servicio Distribuida (DDoS) efectuado por hackers rusos en lenguaje ruso, pero desde una dirección comercial IP en los Estados Unidos[522]. Simultáneamente a la invasión por tierra se ejecutó una segunda ronda de ataques DDoS uno de cuyos primeros objetivos fue un foro en línea de hackers pro georgianos, a los efectos de reducir el número

520 Herr, Military Cyber operations: A primer. Op. Cit.

521 Crowell, Richard M.; Op. Cit.

522 Como resultado, ni Georgia, ni otros investigadores pudieron probar que el gobierno ruso había llevado a cabo estos ataques cibernéticos.

de contraataques contra objetivos rusos[523]. A medida que las tropas rusas avanzaban, los georgianos eran incapaces de acceder a sitios web con información crítica para ellos, como eran las comunicaciones, las redes bancarias y las páginas del gobierno. Adicionalmente, los servicios de telefonía celular cayeron el día después de que el sistema bancario fue anulado.

En enero de 2009, durante la ofensiva sobre la Franja de Gaza, la infraestructura de Internet israelí fue atacada por hackers, especialmente las páginas del gobierno. Fuentes oficiales israelíes manifestaron que el ataque fue llevado a cabo por una organización criminal basada en algún país de la antigua Unión Soviética, financiados por el Hamas o el Hezbollah[524].

El ataque a sus redes de computadoras militares lleva a los Estados Unidos a sospechar que han sido blanco de hackers militares chinos para conocer los programas de despliegue de unidades, la periodicidad de los reabastecimientos, los programas de movimiento de material, las evaluaciones sobre el estado de alistamiento de las unidades, los planes de pre posicionamiento de las unidades navales, las operaciones aéreas de reaprovisionamiento de combustible, y el estado de la logística de las bases en el Teatro Pacífico occidental[525].

Ese mismo año se produjo un ataque cinético sobre las centrifugadoras para enriquecimiento de uranio que los iraníes empleaban en la planta nuclear de Natanz a través del gusano *Stuxnet*.

> Si bien no está claro el efecto general que produjo Stuxnet en el programa nuclear iraní, aunque Irán reconoció el ataque y aparentemente este no modificó la tasa de aumento de las reservas de uranio enriquecido, a partir de finales de 2009 Irán necesitó de más centrifugadoras para llevar a cabo la misma cantidad de trabajo[526].

Para Crowell[527],

> Los acontecimientos de la primavera árabe en Egipto muestran claramente cómo el empleo de códigos y tecnología civil fueron rápidamente adaptados para el uso en el conflicto. Una vez logrado el control y la libertad de acción en el dominio cibernético se pudo alcanzar la libertad de acción en los demás dominios físicos. Esta libertad de acción le permitió en última instancia a la oposición lograr los objetivos físicos de derrotar al régimen de Mubarak. Las operaciones de la oposición egipcia en el domi-

---

523 Theohary, Catherine A. Harrington Anne I.; Cyber Operations in DOD Policy and Plans: Issues for Congress, January 5, 2015 Disponible en: https://fas.org/sgp/crs/natsec/R43848.pdf

524 NATO Review; The history of cyber-attacks - a timeline; Disponible en: http://www.nato.int/docu/review/2013/Cyber/timeline/EN/index.htm.

525 Hay que tener en cuenta que, en determinadas oportunidades, mientras algo que pareciera ser una simple intrusión relacionada con el espionaje y el robo de información sensible, es posible que el malware también pueda llegar a contener una función oculta, más peligrosa, como pudiera ser la capacidad de desactivar las comunicaciones o diseminar desinformación.

526 Albright, David, Brannan, Paul, and Walrond, Christina; Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant? Preliminary Assessment; Disponible en: http://isis-online.org/isis-reports/detail/did-stuxnet-take-out-1000-centrifuges-at-the-natanz-enrichment-plant/

527 Crowel Richard M. Some Principles of Cyber Warfare; The United States Naval War College; Joint Military Operations Department; P. 27

nio terrestre claramente dependían de una fuerza cibernética para obstaculizar a las fuerzas del gobierno; a pesar de haber sido poco convencional.

Sin embargo, a juicio de Luke Coffey[528]

> La guerra en Siria es tal vez la primera guerra civil donde el uso de las redes sociales, Internet, los sistemas masivos de comunicación y las noticias vía satélite han sido utilizados por todas las partes para emprender una campaña de guerra cibernética coordinada.

Para un residente en Gaza, Ashraf Mushtaha[529], experto en seguridad de sistemas de computación,

> Los servicios de inteligencia israelíes usan Internet y las redes sociales para difundir rumores, conducir acciones de guerra psicológica contra el pueblo palestino y reclutar agentes. (Lo hacen) aprovechándose de mal uso que los palestinos hacen de Internet y su laxitud en la apreciación del peligro real que implican las agencias de seguridad israelíes en la Web.

Por su parte, Hamas comprendió rápidamente el impacto potencial que el empleo de los vehículos aéreos no tripulados (UAVs) puede tener en la conciencia pública. En consecuencia, esta organización aprovechando una capacidad tecnológica básica creó un efecto psicológico a través de los diferentes canales de los medios de comunicación en Israel y en todo el mundo. Mientras que la amenaza real de los daños que puede infligir un UAV es menos peligrosa que los misiles o cohetes, los intentos realizados por Hamas para volar un UAV dominaban los encabezados. Esta tendencia a emplear vehículos no tripulados contra el estado de Israel debía continuar en el futuro, como un activo que posee un efecto operacional pero aún más como una estrategia que forma la conciencia[530].

A principios de octubre de 2015, el Ministerio de Defensa ruso informó que se habían realizado 20 incursiones en el primer día de la operación en Siria y bombardeado ocho objetivos en ese país, lo que incluía centros de comando del grupo estado islámico (EI, anteriormente ISIS/ISIL) y depósitos de armas y combustible y que todos los objetivos estaban alejados de las zonas urbanas. Prácticamente al mismo tiempo comenzaron a difundirse informes en las redes sociales afirmando que Rusia no estaba atacando a los terroristas, sino que, por el contrario, los aviones de combate rusos atacaban zonas residenciales y mataban a decenas de civiles.

---

528 Aljazeera net, Coffey, Luke; Syria's online battlefield; 17 junio 2015 Disponible en:http://www.aljazeera.com/indepth/opinion/2015/06/syria-online-battlefield-150617072048625.html.

529 Cyberwar Desk, Hamas' cyber battalions take on Israel; Disponible en: http://cyberwardesk.com/hamas-cyber-battalions-take-on-israel/.

530 Israel Defense Company, Alon Unger; ¿UAVs - A Tactical Resource or a Strategic Asset? Disponible en: http://www.israeldefense.co.il/en/content/uavs-tactical-resource-or-strategic-asset

Mariya Zakharova, portavoz de la Cancillería rusa inmediatamente dijo a la agencia internacional de noticias Reuter[531] que,

> Informes parciales y falsos han inundado occidente y medios regionales diciendo que la operación militar rusa está causando muertes de civiles o incluso que está dirigida contra las fuerzas pro democráticas y la pacífica población. Es un ataque de información, la guerra de la información de la que todos hemos escuchado hablar mucho acerca de ella. Al parecer alguien vino muy bien preparado para ello.

Por otra parte, según Harlan Ullman[532], un miembro en el Consejo Atlántico en Washington, señaló que

> Que las fuerzas armadas de Rusia son capaces de realizar sofisticados bombardeos aéreos y marítimos, en este caso contra militantes islámicos estatales (EI) y otros grupos rebeldes sirios, no es novedoso ni sorprendente. Lo notable es cómo el Kremlin está difundiendo su campaña en Siria. Ha producido videos, imágenes de ataques aéreos desde drones, gráficos animados, fotos sobre el terreno y rápidas actualizaciones de Twitter y Facebook. El Kremlin ha copiado el manual de las operaciones de Washington, abrazando la guerra de la información para el entorno mediático del siglo 21.

Para Nikolai Malishevski[533] *"Esta vez el campo de batalla no son los suburbios de Damasco, de Aleppo ni la frontera sirio-turca, sino más bien el ambiente de información"*.

Durante la operación (*Iraqi Freedom OIF*) se difundieron mensajes desde aviones EC-130E de la Fuerza Aérea y buques de la Armada de los Estados Unidos que operaban en el Golfo Pérsico, junto con un sin número de correos electrónicos, faxes, y llamadas a teléfonos celulares a numerosos dirigentes iraquíes para incitarlos a quitarle el apoyo a Saddam Hussein. Al mismo tiempo, la red de noticias *Al Jazeera*, con sede en Qatar, enviaba sus mensajes a más 35 millones de espectadores en el Medio Oriente[534].

Como un tipo de engaño, durante la operación *Iraqi Freedom* la marina de guerra de Estados Unidos desplegó el sistema táctico aéreo de señuelos para desviar las defensas aéreas iraquíes de los aviones de combate reales[535].

---

531 RT News, Information warfare? Russia accused of killing civilians in Syria; Disponible en: https://www.rt.com/news/317170-russia-accused-civilians-syria/.

532 Radio Free Europe Liberty, Russia's Shock and Awe: Moscow Ups Its Information Warfare in Syria Operation; 7 octubre de 2015, Disponible en: http://www.rferl.org/content/russia-syria-shock-awe-military-air-strikes-information-warfare/27293854.html.

533 Malishevski, Nikolai. Strategic Culture,Syria and Information Warfare; Disponible en: http://www.strategic-culture.org/news/2013/09/23/syria-and-information-warfare.html

534 Wilson, Clay; Information Operations, Electronic Warfare, and Cyberwar: Capabilities and Related Policy Issues; Naval History and Heritage Command; Disponible en: http://www.history.navy.mil/research/library/online-reading-room/title-list-alphabetically/i/information-operations-electronic-warfare-and-cyberwar.html#intro.

535 Ibidem.

Por su parte, la fuerza aérea de Estados Unidos reveló recientemente el uso de un avión EC-130 *Compass Call,* para atacar remotamente las redes enemigas que en la mayoría de los casos podrían estar cerradas, utilizando nuevas técnicas de hackeo[536], "lo cual significa que el ataque también funciona contra Air-gapped computers"[537]. Si bien no se dieron los detalles, esto significa que existe la posibilidad de poder utilizar esta técnica de ataque para hackear redes militares extranjeras desde el aire, evitando muchos de los problemas que significa ingresar en ellas, dado que no permiten el acceso vía USB.

Muchas de esas operaciones también se llevan a cabo en los distintos foros – Twitter, Facebook, - creando espacios en Internet (blogs) para expresar ideas, intereses, experiencias y opiniones o para publicar propaganda a favor de quien contrata los servicios de los denominados "*trolls*"[538] quienes generalmente hablan varias lenguas.

Estas falsas personas parecen ser reales y al ingresar en una discusión a través de blogs, foros, chats, etc. desacreditan a los opositores, o crean la apariencia de un consenso. La técnica utilizada para manipular a la opinión pública *online* es contaminar a mentes inexpertas, y en lo posible a personas que carezcan de formación técnica suficiente para contrastar las novedosas teorías que difunden. Luego esas teorías saltan al plano de los medios de comunicación masivos que difunden los contenidos en forma jocosa, pero que al final terminan ingresando al consciente colectivo.

Cuando alcanzan un nivel de difusión suficiente es el turno de las celebridades, que tienen la facultad de cambiar la opinión del público por medio de una canción, una declaración pública o un mensaje en Facebook o Twitter. De esta manera, termina generándose una dialéctica entre una infinidad de defensores de una teoría, que ni si quiera han leído y comprendido bien.

Al final, los fanáticos convencidos por los *trolls* terminan insultando o acusando de desinformadores a quienes supuestamente dicen la verdad.

Según la BBC[539] en 2014, Rusia ha visto un aumento sin precedentes en la actividad de los llamados *"Trolls del Kremlin"* – que son bloggers supuestamente pagados por el estado para criticar a Ucrania y a occidente en las redes sociales y publicar comentarios favorables sobre el liderazgo de Moscú. Una investigación realizada le asigna a Yevgeny Prigozhin, un restaurador con estrechos vínculos con el Presidente Vladimir Putin, a contratar *bloggers* para producir cientos de comentarios en los principales sitios web de noticias y administrar varias cuentas en Twitter, *LiveJournal* y otras plataformas de medios sociales.

---

536 Security Affairs, The US Air Force is using a modified EC-130 Compass Call aircraft to demonstrate how to hack into enemy networks. Disponible en: http://securityaffairs.co/wordpress/40600/hacking/us-air-force-flight-hacking.html

537 Es una medida de seguridad de la red también conocida como separaciones de aire, que emplea uno o más equipos para asegurar que una red informática segura esté físicamente aislada de redes sin garantía, como la conexión a Internet o a una red de área local no segura. El nombre deriva de la técnica de crear una red que no tiene y a menudo nunca ha tenido, una conexión insegura activa, por tener los dos computadores físicamente separados, con aire en el medio.

538 Usuarios cuyo único interés es molestar a otros e interrumpir el correcto desempeño de un foro, ya sea por no estar de acuerdo con su temática o simplemente para publicar propaganda a favor de quien los ha contratado.

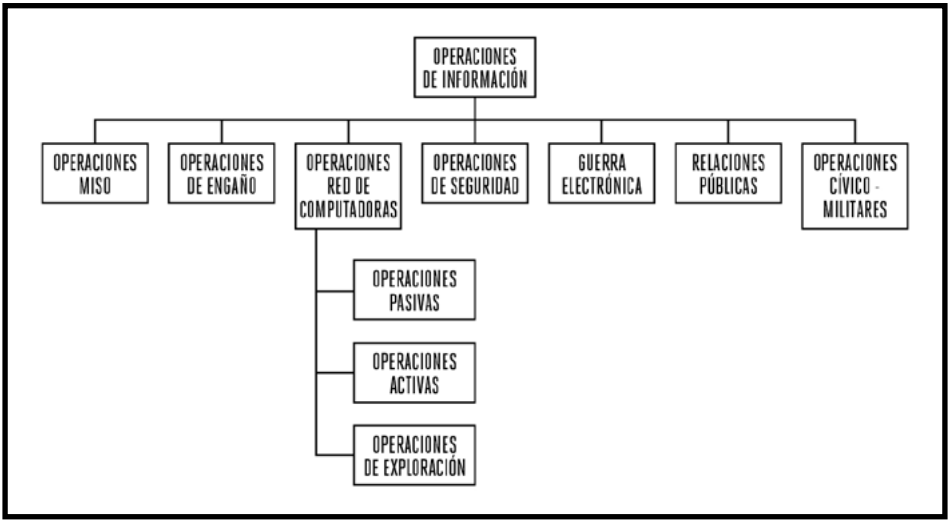
539 BBC News, Olga Bugorkova; Ukraine conflict: Inside Russia's 'Kremlin troll army; 19 marzo 2015 Disponible en: http://www.bbc.com/news/world-europe-31962644.

Lo descripto hasta ahora puede resumirse en que las operaciones cibernéticas son el empleo de las capacidades del ciberespacio con el propósito principal de lograr objetivos en o a través de él.

Por su parte, las operaciones de información son el empleo integrado, durante las operaciones militares, de las capacidades relacionadas con la información en concierto con otras líneas de operación para influir, alterar, corromper o usurpar la toma de decisiones de adversarios y potenciales adversarios al mismo tiempo que se protegen las propias. A diferencia de otros efectos que se pretenden alcanzar en el campo de batalla, se centran en tratar de influir en las percepciones o actitudes de quienes deben tomar decisiones en lugar de destruir cosas o ganar terreno.

Cuando las capacidades cibernéticas se emplean en apoyo de las operaciones de información, el efecto que se pretende lograr es negar o manipular la toma de decisiones del adversario o de un potencial adversario, impactando sobre un medio de información (como un punto de acceso inalámbrico en la dimensión física), el mensaje propiamente dicho (un mensaje cifrado en la dimensión de la información), o a una cyber-persona (una identidad en línea que facilita la comunicación, toma de decisiones y la influencia de las audiencias en la dimensión cognitiva). Cuando se emplea en apoyo de las operaciones de información, generalmente se centran en la integración de capacidades ofensivas y defensivas ejecutadas en y a través del ciberespacio, en concierto con otras capacidades relacionadas con la información y en coordinación a través de las líneas de operación y de las líneas de esfuerzo.

FIGURA 13: OPERACIONES DE INFORMACIÓN[540]



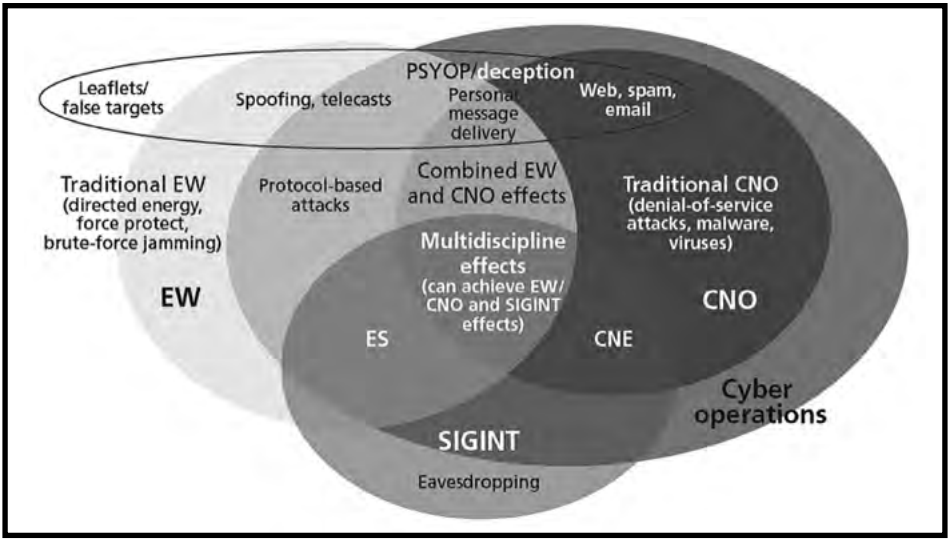
540 Elaboración propia

Las capacidades relacionadas con la información son las herramientas, técnicas y actividades que pueden ser utilizadas dentro del ambiente de la información para crear un efecto deseado sobre una audiencia específica. Pueden incluir, sin que esto sea limitativo, una variedad de actividades técnicas y no técnicas que entrecruzan las áreas tradicionales de las operaciones de apoyo de información militar (MISO), el engaño militar (MILDEC), las operaciones de red de computadoras, la seguridad de las operaciones (OPSEC), de guerra electrónica y otras.

Si se toma como categoría de orden el efecto que producen, estas operaciones de información pueden identificarse en cuatro formas: sobre el comando y control; sobre los datos para el mejor desarrollo de las operaciones en el terreno; sobre los medios electrónicos que se usan; sobre la mente de los individuos en sus diferentes roles; y sobre los medios cibernéticos. Todas estas formas se llevan a cabo para facilitar las propias operaciones, y para dificultar las del oponente, y se llevan a cabo en los ámbitos físicos, informativos y los pertenecientes al conocimiento individual. Estas clasificaciones no son absolutas, en muchas partes estas categorías se superponen y es por eso que es difícil encontrar una definición ideal.

La figura 14 proporciona una vista funcional de las relaciones y los límites entre la guerra electrónica (óvalo amarillo), la inteligencia de señales (SIGINT) (óvalo azul), las operaciones de red de computadoras (óvalo violeta) y las operaciones cibernéticas (óvalo rojo).

FIGURA 14: VISTA FUNCIONAL DE ÁREAS CONVERGENTES[541]



541 Porche, Isaac R. III, Paul, Christopher, York, Michael, Serena, Chad C., Sollinger, Jerry M., Axelband, Elliot, Min, Endy Y., Held, Bruce J. Redefiing Information Warfare Boundaries for an Army in a Wireless World, RAND Corporation, P. 51. Disponible en: http://www.rand.org/content/dam/rand/pubs/monographs/MG1100/MG1113/RAND_MG1113.pdf

Como puede verse, hay funciones que se encuentran en un único dominio: para la guerra electrónica, por ejemplo, el jamming; para SIGINT, la escucha; pero para las operaciones cibernéticas, se aprecia un conjunto de posibilidades (por ejemplo, web y correo electrónico de spam, ataques de denegación de servicio, malware, virus). Las operaciones MISO (anteriormente operaciones psicológicas) y de engaño (MILDEC) se muestran también en el óvalo aplanado en la parte superior de la figura, en la intersección entre las operaciones cibernéticas y de guerra electrónica, que únicamente contiene panfletos y falsos blancos.

Considerando todos estos ejemplos, y tomando como categoría de orden el efecto que producen en esa intersección entre las redes sociales y el espacio cibernético, de la que se hablara anteriormente, pueden identificarse cinco formas de operaciones de información cibernéticas: sobre el comando y control; sobre los datos para el mejor desarrollo de las operaciones en el terreno; sobre los medios electrónicos que se usan; sobre la mente de los individuos en sus diferentes roles; y sobre los medios cibernéticos[542]. Esto, en relación con las operaciones militares, se traduce en operaciones de apoyo de información militar (antiguamente llamadas operaciones psicológicas), operaciones de engaño, de seguridad cibernética militar, operaciones de red de computadoras y operaciones de guerra electrónica.

FIGURA 15: VISTA GENERAL DE LAS OPERACIONES DE INFORMACIÓN[543]

Visión general de las operaciones de información		
Operaciones de apoyo de información militar MISO / Op. Psicológicas	> Monitoreo y manipulación de sentimientos > Campañas de contra propaganda > Panfletos electrónicos / Difusión de información > Ingeniería social	> Penetración de medios de comunicación social > Mal direccionamiento > Respuesta a eventos o incidentes > Desfasaje de sitios Web
Engaño militar	> IP *Spoofing* > Manipulación de imágenes digitales > Alteración de archivos de computadoras	> Almacenaje falso de archivos > Archivos electrónicos engañosos > Señuelos (*Honey spots*)

»

542 de Vergara, Evergisto. Implementar Estrategias, Capítulo XVI. En: Las Operaciones de Información Disponible en: www.IEEBA.com. (Escrito por uno de los autores de esta investigación, el Gral. de Div. (R) Evergisto de Vergara).

543 Slideshare Inc, Cyber Overview on Information Operations, Disponible en http://www.slideshare.net/lkcyber/cyber-overview-of-information-operations.

»

Operaciones militares de seguridad cibernética (OPSEC)	> Administración de activos cibernéticos > Clasificación de la información y Control de acceso > Administración de las comunicaciones > Adquisición, desarrollo y mantenimiento de sistemas	> Manejo de incidentes > Evaluación de riesgos cibernéticos > Seguridad de la información
Operaciones de red de computadoras	> Ataque de red de computadoras (CNA) > Defensa de la red de computadoras (CND) > Explotación de red de computadoras (CNE)	> Operaciones cibernéticas defensivas (DCO) > Operaciones cibernéticas ofensivas (OCO) > Defensa de las redes de información (DODIN)
Guerra electrónica	> Ataque ciberelectrónico > Protección ciberelectrónica > Apoyo cibernético a la guerra electrónica	

Como fuera dicho, las operaciones de información buscan perturbar o influir en los procesos de toma de decisiones del adversario. Teniendo en cuenta los ejemplos expuestos y el contenido de la figura 15, se observa con claridad que las operaciones de información cibernética pueden tomar muchas formas que van desde la interferencia a señales de radio y televisión, el secuestro de emisiones de estos medios de comunicación para llevar a cabo campañas de desinformación, la inhabilitación de redes logísticas, el espionaje dentro de las redes de computadoras de un adversario hasta el sabotaje de sistemas bancarios. Asimismo, puede tratarse de la interrupción o disminución de la velocidad de los sistemas del adversario mediante la transmisión de un virus u otros códigos maliciosos o bien el desvío de sensores enemigos, para crear falsas imágenes. Otros métodos de ataque de operaciones de información podrán incluir operaciones psicológicas como iniciar transmisiones de radio y televisión para influir en las opiniones y acciones de una audiencia, o apoderarse del control de las comunicaciones de red para alterar la unidad de comando del adversario.

Ya definidas las operaciones de información, su interrelación con las operaciones cibernéticas y su aplicación en diferentes conflictos, en el siguiente punto se esbozarán algunas sugerencias para su incorporación al planeamiento de una campaña.

Las operaciones de información en el planeamiento operacional

En el proceso de planeamiento conjunto estadounidense, la planificación de las operaciones de información suele ser un esfuerzo de apoyo. Si se suscribe a la idea de que todas las guerras se libran en el plano cognitivo, al menos en algún punto, es lógico asumir

que, en un momento u otro, los cursos de acción (COAs) de la guerra de información deben ser el esfuerzo apoyado. Más aun, muchas veces los "temas de las operaciones de apoyo a las operaciones de información" (MISO) se desarrollan después de los cursos de acción de las operaciones militares cinéticas[544].

Según Robert R. Reilly[545],

> Para que una operación de información sea exitosa deberá entenderse al público objetivo, tener el mensaje correcto en el formato adecuado para llegar a ese público y los elementos para entregar el mensaje a través de los medios de comunicación utilizados por el público.

En consonancia con ello, para la doctrina brasilera[546], en el planeamiento dentro del nivel estratégico militar puede verse que las Operaciones de Información tienen como finalidad.

> Coordinar y sincronizar los sistemas de comunicación estratégica, con el propósito de desarrollar ideas-fuerza a ser difundidas a públicos seleccionados, no afectando a la seguridad nacional o la seguridad de las operaciones en zonas de crisis o de conflicto armado.

Dicho planeamiento prevé que el Anexo correspondiente al de las Operaciones de Información contenga los siguientes apéndices: Operaciones Psicológicas, Comunicación Social, Guerra Electrónica y Defensa Cibernética.

A su vez, en el punto 8 del Plan de Campaña[547], para la misma doctrina, el Comandante Operacional debe:

> Presentar toda la información y directrices relacionadas a las actividades de los medios de comunicación, operaciones psicológicas, guerra electrónica y ciberdefensa. Debido al volumen de información normalmente se preparará una información de las operaciones, con anexos específicos para cada actividad, y este artículo sólo hará referencia a la misma.

La doctrina de los Estados Unidos describe a las operaciones de información como el

---

544 Gery, William R., Lee, SeYoung and Ninas, Jacob Information Warfare in an Information Age JFQ 85, 2nd Quarter 2017, P. 25. Disponible en: http://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-85/jfq-85.pdf

545 Westminster Institute, Robert R. Reilly; Information Operations: Successes and Failures; febrero 2015, Disponible en http://www.westminster-institute.org/articles/information-operations-successes-and-failures/

546 Brasil. Ministério Da Defesa; MD41-M-01; Doutrina de Operações Conjuntas 1o Volume; 1ª Edição 2011; Adendo 3ao Apêndice IIao ANEXO B Modelo De Plano Estratégico de Operações de Informação (PEOI) P. 108/128. Disponible en http://www.esg.br/images/manuais/Manual%20de%20Doutrina%20de%20Operacoes%20Conjuntas%20-%201%C2%BA%20Volume.pdf.

547 Ibídem.

uso integrado, durante operaciones militares, de herramientas, técnicas y actividades empleadas dentro de una dimensión del ambiente de la información que pueden utilizarse para alcanzar un fin específico, en concierto con otras líneas de operación para influir, alterar, corromper o usurpar la toma de decisiones de adversarios y potenciales adversarios al mismo tiempo que se protegen las propias[548].

Como detalla Wentz[549]:

> La conducción de las Operaciones de Información (IO) requiere la integración estricta y continua de las capacidades y actividades ofensivas y defensivas, como así también el eficaz diseño, integración e interacción de C2 con apoyo de inteligencia. Las capacidades ofensivas más importantes de la Operación de Información (IO) incluyen, pero no se limitan a los elementos de la guerra de C2 (C2 W), como la Seguridad de las Operaciones (OSPEC), las operaciones psicológicas (PSYOP), la decepción militar, la Guerra Electrónica (EW), la destrucción psicológica y el ataque de las redes de computación (CNA). Las capacidades defensivas de las Operaciones de Información (IO) incluyen la seguridad física, la contra decepción, las contra-PSYOP (también denominadas contra propaganda), el contraespionaje y la protección electrónica. Las actividades relacionadas con las Operaciones de Información (IO) incluyen la garantía de la información (IA), los asuntos públicos (PA) y los asuntos civiles (CA). La garantía de la información (IA) protege y defiende la información y los sistemas de información garantizando su disponibilidad, integridad, identificación y autenticación, carácter confidencial y aceptación. También incluye el restablecimiento de los sistemas de información incorporando las capacidades de protección, detección, reconstitución y reacción. Los asuntos públicos (PA) comunican información precisa, equilibrada y creíble a los líderes críticos y el público. Los asuntos civiles (CA) establecen relaciones entre las fuerzas militares, las autoridades públicas y civiles para intercambiar información, preparar un entendimiento y ganar información.

Para Libicki,[550] las operaciones de información

> ...son muy difíciles de llevar a cabo sin el conocimiento preciso y confiable de la arquitectura de la otra parte: desde cómo los medios de información y noticias influyen en sus decisiones, hasta la estructura burocrática del comando, la infraestructura de comunicaciones de la nación y el detalle del software de sus sistemas de información.

---

548 Joint Publication 3-13, Information Operations, Dated 27 November 2012 Incorporating Change 1, 20 November 2014

549 Wentz, Larry. K., Operaciones de Información de Coalición: la experiencia IFOR, Disponible en: http://argentina.afceachapters.org/wp-content/uploads/2013/11/OPERACIONES2.pdf

550 Libicki Martin C.; What Is Information Warfare? Strategic Forum; Number 28, May 1995; Disponible en: https://www.questia.com/library/journal/1G1-129891565/what-is-information-warfare.

En el nivel operacional, los planificadores piensan primero en términos de efectos específicos que quieren tener sobre un adversario (degradar, demorar, destruir, alterar, desviar, neutralizar y suprimir) y luego en las herramientas que tienen a su disposición y cómo pueden utilizarlas para lograr el efecto deseado. En otras palabras, ¿qué efecto quieren obtener, y en quién (o qué) quieren lograr esos efectos?

Según la publicación *Introduction to Operations and Planning*[551], las operaciones de información pueden crear efectos estratégicos (tanto deseados como no deseados), incluso cuando son empleados en el nivel de la fuerza conjunta o de un componente. Por ello, deberían apoyar los objetivos del Comandante del Teatro:

- Transmitiendo información seleccionada e indicadores a determinadas audiencias.
- Ayudando a dar forma a las percepciones de los tomadores de decisiones.
- Ayudando a preservar la información propia (particularmente en el ciberespacio)
- Protegiendo contra el espionaje.
- Protegiendo contra el sabotaje y otras actividades de colección de inteligencia del adversario.
- Comunicando una adecuada información no clasificada sobre las actividades propias.

A modo de ejemplo, la publicación muestra los siguientes efectos que podrían lograrse:

- Obstaculizar la capacidad de atacar de un adversario creando confusión en el ambiente operacional.
- Frenar o detener el tempo operacional del adversario causándole dudas, confusión y mal direccionamiento de la información.
- Reducir la capacidad de comando y control (C^2) de un adversario mientras que se facilita la transición de la guerra a la paz.
- Utilizar las capacidades de las operaciones de información en lugar de la destrucción física para prevenir o disminuir los costos de reconstrucción durante la transición de la guerra a la paz.
- Influir en la percepción de los líderes del adversario y neutrales, en las fuerzas militares y en las poblaciones respecto de los objetivos propios.
- Alterar los planes del adversario, potenciando así los planes y operaciones propios.
- Impactar negativamente sobre la capacidad de liderazgo del adversario afectando sus comunicaciones o la comprensión del entorno operativo.
- Perturbar la capacidad del comandante adversario para enfocarse en el poder de combate.
- Influir en la estimación de la situación del comandante adversario.
- Conducir operaciones de información que reduzcan las vulnerabilidades del ambiente físico a los ataques del ciberespacio.

---

551 Introduction to Operations and Planning, Last Updated: 04 November 2016, P. 140. Disponible en: https://doctrine.af.mil/download.jsp?filename=3-0-D01-OPS-Introduction.pdf

- Proteger de las fuerzas durante las operaciones humanitarias de las amenazas asimétricas.

Acto seguido, la pregunta que deberían hacerse los planificadores, tendría que enfocarse en ¿cómo aprovechar las ventajas que brinda el espacio cibernético para lograr el efecto deseado?

En primer lugar, la planificación de las operaciones de información y el empleo de las capacidades relacionadas requieren apoyo de inteligencia. La preparación de inteligencia del espacio de la batalla (IPB) es un proceso continuo para desarrollar un conocimiento detallado de los adversarios, tanto en el Teatro de Operaciones como en el ambiente de la información. Ese apoyo de inteligencia se encuentra basado en el IPB tradicional, y para las operaciones de información requiere lo siguiente:

- En la dimensión física, una comprensión de los elementos humano, técnico y de infraestructura que apoyan el contenido y el flujo de información.
- En la dimensión informativa, un conocimiento del contenido de información y cómo fluye la información hacia y desde un adversario y otros.
- En la dimensión cognitiva, la comprensión de las influencias políticas, sociales y culturales del potencial adversario, su proceso de toma de decisiones, sus factores de motivación, su estilo de liderazgo y las consideraciones políticas y militares que restringen su radio de acción.

En lo que respecta a las operaciones de apoyo de información militar (MISO), antiguamente denominadas operaciones psicológicas, a través de Internet, o vía mensajes de celulares, una información puede ser enviada de manera instantánea antes de que pueda ser adjudicada su autenticidad. Los teléfonos móviles pueden ser el medio a través del cual se pueden enviar mensajes normales, en forma de noticias, desacreditar líderes u ofrecer un punto de vista diferente sobre la situación.

En "*Cyber Silhouettes: Shadow over Information Operations*" el autor, Timothy Thomas, señala que existe un colapso de los grandes medios. La sociedad como un todo está confiando más en los productos virtuales que en los periódicos y otras formas de impresión.

Grupos como Al-Qaeda y Hezbollah han desarrollado operaciones psicológicas intentando cambiar las actitudes y comportamientos a través de la intimidación, el miedo u odio racial o religioso. Algunas de ellas no solo se dirigen hacia el público externo, sino también al interno, descontentos por la situación o por haber sido marginados durante el reclutamiento[552].

Para Baker[553],

---

552 Thomas, Timothy L. Hezbollah, Israel, and Cyber PSYOP, Winter 2007, Disponible en: http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA465336.

553 Baker, Prentiss O., Psychological Operations Within the Cyberspace Domain, Disponible en: www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA519576

La cibernética y las tecnologías persuasivas ofrecen varias ventajas. En primer lugar, son interactivas lo que les permite desarrollar planes en función de cómo evoluciona la situación y basados en un público determinado. En segundo lugar, en el dominio cibernético estas tecnologías persuasivas pueden ser más persistentes que los seres humanos. Las máquinas pueden trabajar día y noche para convencer a un individuo. En tercer lugar, pueden ofrecer mayor anonimato lo cual permite que el objetivo supere las fuerzas sociales y la cultura rutinarias, haciéndolo más susceptibles a las técnicas de influencia. En cuarto lugar, la información que se presenta para influir a la audiencia puede ser fácilmente modificada y cambiada en el dominio de la cibernética. Por último y quizás lo más importante es que estas tecnologías persuasivas a través del dominio de la cibernética pueden ir donde los seres humanos no pueden ir o no ser bienvenidos.

Baker señala algunos puntos de vista mediante los cuales un Comandante de Teatro puede ser capaz de tomar rápidas decisiones y redistribuir el poder dentro del espacio cibernético, a fin de disminuir la capacidad del adversario al mismo tiempo que mejora la suya para adaptarse como un todo orgánico, de manera que el oponente no pueda hacer frente mientras que él puede afrontar con esfuerzos / eventos a medida que se desarrollan.

Asimismo, en lo que a operaciones psicológicas se refiere, Baker[554] afirma que,

...desde la perspectiva de las operaciones psicológicas, el foco está en penetrar al adversario para disolver su fibra moral, desorientar sus imágenes mentales, interrumpir sus operaciones y sobrecargar su sistema, así como subvertir, capturar los bastiones morales, mentales y físicos, las conexiones o actividades que dependen de ellos, con el fin de destruir la armonía interna, producir parálisis y colapsar su deseo de resistir.

Para Martin C. Libicki[555]

Las operaciones cibernéticas pueden apoyar a las operaciones MISO de varias maneras. Dispositivos y sitios web pueden ser infectados para llevar a los usuarios a una propaganda que muestra lugares inesperados o lleva identificaciones inesperadas[556]. Comprometiendo determinados sistemas se puede llevar a la gente a sitios a los cua-

554 Baker, J; Psychological Operations Within the Cyberspace Domain; Op. Cit.

555 Libicki, Martin C., The Convergence of Information Warfare Strategic Studies Quarterly • Spring 2017, P. 51, Disponible en: http://www.airuniversity.af.mil/Portals/10/SSQ/documents/Volume-11_Issue-1/Libicki.pdf

556 Después que el Tribunal de la Haya fallara en contra de China sobre cuestiones de soberanía con las Filipinas en el mar de China meridional, altavoces y pantallas mostraron la bandera nacional en las pantallas de Vietnam Airlines de dos aeropuertos de Vietnam en las ciudades de Hanoi y ciudad Ho Chi Minh. Mensajes ofensivos y lo que fue descrito por los medios estatales como "información distorsionada" sobre Vietnam y los reclamos de las Filipinas sobre el mar de China meridional fueron mostradas en las pantallas de información de vuelo. Aunque el fallo fue a favor de las Filipinas, las aguas son disputadas también por Vietnam, con lo cual, cualquier ganancia contra China por uno de los reclamantes es una pérdida para los otros.

les no tenían intención de ir o que falsamente pretenden ser donde tenían la intención de hacerlo. Técnicas similares se pueden y se utilizan para mejorar el ranking de credibilidad de la página de sitios favoritos. *Spam-bots* puede ser diseñados para dominar debates en línea[557]. Material robado a opositores políticos pueden ser tergiversados con documentos amañados con apropiados niveles de verosimilitud.

Los mensajes no tienen que convencer (por ejemplo, comprar esto, creo que); en un contexto de conflictos, el objetivo es inducir miedo o por lo menos ansiedad y así paralizar la resistencia de una persona a la vez; adaptar los mensajes a cada persona erosiona la solidaridad de los grupos que enfrentan la misma amenaza.

En cuanto al engaño cibernético deberá tenerse en cuenta que es diferente del clásico engaño militar pues en este caso el objetivo podría ser tanto quien toma una decisión como un sistema electrónico en la red del adversario. Por ejemplo, un defensor de la red podría intentar engañar un malware, modificando la configuración de una computadora virtual para intentar inducir al software que se ejecuta directamente en el hardware y mejorar la capacidad para analizarlo[558].

En la figura 16, pueden apreciarse los distintos efectos que tanto un atacante como un defensor pueden lograr con el engaño cibernético.

FIGURA 16: EJEMPLOS DE ENGAÑO CIBERNÉTICO[559]

Fallar en el análisis	Impedir que el defensor detecte el ataque.	Evitar que el atacante descubra su blanco.
Revelar	Engañar al defensor para que le permita el acceso.	Engañar al atacante para que revele su presencia.
Perder el tiempo	Desviar la atención del defensor hacia aspectos equivocados del incidente	Concentrar los esfuerzos del atacante en un objetivo equivocado.
Subestimar	Inducir al defensor para que crea que el ataque es sencillo, y no dirigido.	Inducir al atacante a pensar que lo que busca no está allí.

»

557 Durante las protestas de Maidan en Ucrania en 2013 – 2014, los 'spam bots' rusos tenían una presencia mucho mayor en los Twitters de Ucrania que los tweets de la oposición rusa.

558 Cross, Tom. Deception for the Cyber Defender; Disponible en: https://shmoo.gitbooks.io/2015-shmoocon-proceedings/content/bring/02_deception_for_the_cyber_defender.html

559 Ibidem.

Desentender	Inducir al defensor a pensar que el ataque está contenido o completado.	Inducir al atacante a pensar que ya ha logrado su objetivo.
Mal direccionar	Desviar la atención del defensor hacia otro atacante.	Inducir al atacante a atacar a una víctima diferente.
Desatribuir	Inducir al defensor a pensar que el atacante es alguien más.	Inducir al atacante a pensar que ha comprometido la red equivocada.

Según la publicación *Joint Publication 3-13.4 - Military Deception*, las funciones de las operaciones de engaño incluyen:

- Causar ambigüedad, confusión o mala interpretación en las percepciones que el adversario tiene sobre la información crítica propia;
- Hacer que el adversario ubique incorrectamente a su personal, sus recursos y sus materiales de manera que sean ventajosos para la fuerza propia;
- Hacer que el adversario revele sus fortalezas, disposición de sus fuerzas y futuras intenciones;
- Condicionar al adversario a patrones particulares de comportamiento de las fuerzas propias para inducir sus percepciones, de manera tal que puedan ser explotadas por la fuerza conjunta.

En diciembre de 2014, Ucrania entregó a Estados Unidos fotografías tomadas en Georgia en 2008, como prueba de que Rusia había invadido Ucrania, en una de las cuales aparece una columna de tanques rusos. Basándose en esas "pruebas" el senador estadounidense Jim Inhofe presentó el proyecto de ley que habría de permitir a Estados Unidos enviar armas a Ucrania para contrarrestar los tanques rusos que aparecían en las fotos.

> Las imágenes fueron entregadas por miembros del parlamento ucraniano a la comisión de defensa del senado estadounidense por una delegación ucraniana y el senador se sintió "seguro" de hacerlas públicas, porque, según él, las fotos "coincidieron con los informes" sobre la situación en Ucrania, explicó el director de comunicaciones del congresista, Donelle Harder, citado por el portal 'Free Beacon' que inicialmente las publicó como exclusiva y luego reconoció su error[560].

En lo que respecta a las operaciones militares de seguridad cibernética, para el De-

560 Tecnology Militar. Furia en Washington por las fotos falsas de tanques rusos en Ucrania que aportó Kiev sábado, 14 de febrero de 2015, Disponible en: http://tecnologamilitar.blogspot.com/2015/02/furia-en-washington-por-las-fotos.html#6tiHVExMA5vVQbAk.99

partamento de Defensa de los Estados Unidos[561] constituyen un proceso de identificación de la información crítica y el análisis de acciones amigables relacionadas con las operaciones militares y otras actividades para:

a. Identificar aquellas acciones que pueden ser observadas por los sistemas de inteligencia del adversario.
b. Determinar los indicadores y vulnerabilidades que podrían obtener los sistemas de inteligencia del adversario para poder interpretar o reunir información crítica oportuna para usar contra Estados Unidos y / o las misiones, y que plantea un riesgo inaceptable.
c. Seleccionar y ejecutar las medidas que eliminan el riesgo de operaciones y acciones amigables o reducirlas a un nivel de riesgo aceptable.

Para Guillem Colom[562]

> Aunque muchas fuerzas armadas se han subido al carro de las redes sociales de forma más o menos efectiva y con una estrategia más o menos clara con el objetivo de mejorar su comunicación estratégica, el uso personal que sus integrantes hacen de las mismas puede suponer tanto una amenaza para la seguridad nacional y un riesgo para las operaciones militares como representar un problema de comunicación pública.

En este sentido, las Fuerzas de Defensa de Israel (FDI) son un buen ejemplo de ello. Aunque estas constituyen el ejemplo paradigmático del uso y explotación de las redes sociales, también están sufriendo varios problemas de difícil solución. De hecho, según sus propias estimaciones, aproximadamente el 70 por ciento de sus oficiales y suboficiales y el 95 por ciento de su tropa disponen de perfil personal en Facebook. No obstante, su uso inadecuado provocó que en el año 2013 se prohibiera a los soldados pertenecientes a unidades de inteligencia de operaciones especiales compartir en las redes sociales virtuales fotografías que revelasen su condición de militar, máxime tras algunos episodios que pusieron en peligro la seguridad del país y la reputación de sus Fuerzas Armadas. El servicio de mensajería instantánea *Whatsapp* también ha sido una importante fuente de problemas para las Fuerzas de Defensa de Israel (FDI) y no debe descartarse que esta aplicación o sus equivalentes Telegram o Line puedan plantear graves problemas de seguridad para sus usuarios militares.

Además, las redes sociales virtuales también pueden ser utilizadas por los soldados como medio de protesta. Por ejemplo, el pasado mayo una campaña realizada a través de Facebook de apoyo a un soldado israelí arrestado tras ser grabado mientras apuntaba con su arma a dos adolescentes palestinos en Cisjordania consiguió más de 120.000 "Me gusta".

---

561 Headquarters Department of the Army Washington, DC 26 September 2014AR 530–1 Operations Security, Disponible en: https://fas.org/irp/doddir/army/ar530-1.pdf

562 Guillem Colom; Ciber Elcano, Informe mensual de ciberseguridad Op, Cit.

Del mismo modo, durante la escalada militar en Ucrania, el inadecuado uso de las redes sociales por parte de soldados rusos ha comprometido la Seguridad de la Operación (OPSEC) y puesto en duda la versión oficial de Moscú sobre su no implicación en el conflicto.

En este sentido, las fotografías compartidas por el soldado Alexander Sotkinen en su cuenta de Instagram lo geolocalizaban dentro de las fronteras ucranianas, más concretamente entre los pueblos de Krasna Talycha y Krasny Derkul, ambos controlados por las fuerzas rebeldes. Otros soldados, como Vladislav Laptev o Mikhail Chugunov publicaron en su perfil de VKontkte – una red social rusa similar a Facebook – fotografías de los convoyes militares rusos desplazándose a la frontera ucraniana o declaraciones de que "dispararon toda la noche contra Ucrania", tal y como confirmó posteriormente la inteligencia estadounidense mediante fotografías de satélites.

No obstante, puede que el caso más conocido y controvertido de los riesgos – en este caso estratégicos y políticos – que entraña el empleo de las redes sociales para la seguridad de las operaciones militares es el caso de Igor Girkin, líder separatista de la autoproclamada República Popular de Donetsk, felicitándose en la red social Vkontkte de haber abatido un avión de transporte ucraniano Antonov AN-26 cerca de la ciudad de Torez; un avión que resultó ser el vuelo MH-17 de Malaysia Airlines y en el que murieron trescientos pasajeros. Un capítulo aparte merecería el análisis de inteligencia empleando fuentes abiertas como redes sociales virtuales, fotografías y herramientas de geolocalización para identificar y situar al lanzador autopropulsado del misil superficie aire SA-11 (que formaba parte del sistema antiaéreo BUK) que derribó este avión.

El citado Director de THIBER Guillem Colom Piella, culmina su artículo señalando que:

> El empleo de las redes sociales en el ámbito militar no sólo se ha convertido en una importante herramienta de comunicación estratégica, sino también en una amenaza para la seguridad de las operaciones militares, un altavoz para las protestas de los soldados y un riesgo para la imagen y reputación de sus fuerzas armadas.

La Armada de los Estados Unidos, en diciembre de 2016, a través del Secretario de Marina, promulgó la Directiva 072/16 implementando nuevas políticas de OPSEC[563] las cuales incluyen dos recursos útiles: una herramienta de auto inspección y una lista de información crítica (CIL). La herramienta de auto inspección está diseñada para facilitar una evaluación interna para determinar el cumplimiento de los estándares del Departamento de Defensa (DOD) y Departamento de la Armada (DON) así como, proporcionar a los comandos de nivel superiores la capacidad de evaluar la efectividad de los programas subordinados. La Lista de información crítica de DON (CIL) proporciona una visión general de lo que el Secretario de la Armada considera "información crítica"

563 Navy New OPSEC Policy, Disponible en: http://www.military.com/military-report/navy-new-opsec-policy.html

en el Departamento. Cada comando debe a su vez desarrollar su propia lista basado en amenazas operacionales locales y específicas.

Por lo general, la "información crítica" es información sensible que no necesariamente posee algún grado de clasificación, como, por ejemplo: ejercicios de adiestramiento, composición y disposición de las fuerzas, redes de computadoras, restricciones logísticas, tipos y capacidades de medios para colectar inteligencia, entre otras. Es por ello que todo el personal debe entender la capacidad del adversario para recopilar información y tomar las adecuadas contramedidas de seguridad para negarle el uso de esa capacidad.

En el planeamiento, la "Lista de Información Crítica" constituye un agregado al apéndice de Operaciones de Información, del anexo Operaciones del Plan de Campaña o de una orden de operaciones.

Sirve de ejemplo la destrucción de helicópteros de ataque AH-64 "Apache", del ejército de Estados Unidos, en 2007:

> ...los sucesos ocurren cuando unos soldados suben a Internet unas fotos de la nueva dotación de vehículos aéreos en una base de Irak apareciendo en los metadatos las coordenadas geográficas de la misma. El resultado de dicha filtración involuntaria fue la pérdida de cuatro unidades al ser utilizada la información por fuerzas insurgentes para llevar a cabo un ataque con morteros[564].

¿Qué hacer? En cuanto a la defensa pasiva, la compartimentación de redes y la promoción de la resiliencia pueden reducir la cantidad y calidad de los datos disponibles, disminuyendo así el valor de la penetración. Invertir en la redundancia de la red también puede ayudar a mantener apartadas de los atacantes partes vitales de la red y reducir el tiempo en que una red está fuera de servicio. El uso de máquinas de escribir[565] para las comunicaciones sensibles también puede reducir la exposición.

En cuanto a la defensa activa, Alexander Vipond[566] recomienda tener equipos de respuesta a emergencias informáticas bien entrenados y bien dotados de recursos. Cuanto más rápido se pueda detectar, mitigar y neutralizar un hackeo menor será el daño que puede hacer en el ambiente cibernético y en las relaciones públicas. También, es importante rastrear al culpable, mediante un adecuado análisis forense de intrusiones, a fin de que quede en evidencia y de esa manera poder desacreditar su relato.

En lo que respecta a la guerra electrónica cibernética, que es una forma de guerra electrónica, es necesario comprender que no es lo mismo que la guerra cibernética, aunque existan similitudes entre ambas.

---

564 USAA. 5 Social Networking Tips for Military Members Disponible en: https://www.usaa.com/inet/pages/advice-security-socialnetworkingmilitary?akredirect=true

565 Lyons,Siobhan; Typewriters are back, and we have Edward Snowden to thank; Disponible en: https://www.washingtonpost.com/posteverything/wp/2014/11/12/typewriters-are-back-and-we-have-edward-snowden-to-thank/?utm_term=.5dce58e975c5

566 Vipond, Alexander Understanding the Cyber Threat: Defence, Response, Democracy, Australian Strategic Policy Institute, 6 Feb 2017, Disponible en: https://www.aspistrategist.org.au/understanding-cyber-threat-defence-response-democracy/?utm_medium=email&utm_campaign=Daily%20The%20Strategist&utm_content=Daily%20The%20Strategist+CID_5b2c66017d55f36455c4e623d035156f&utm_source=CampaignMonitor&utm_term=Understanding%20the%20cyber%20threat%20defence%20response%20democracyShare

La guerra electrónica incluye la acción militar que involucra el uso de la energía electromagnética dirigida para controlar el espectro electromagnético o para atacar al enemigo. Las operaciones de guerra electrónica y las operaciones cibernéticas son complementarias y tienen efectos sinérgicos. Por ejemplo, el empleo de un sistema de armas aerotransportado para entregar un código malicioso al ciberespacio a través de una conexión inalámbrica se caracterizaría como un ataque de red de computadoras entregada por medio de la guerra electrónica.

Los límites entre las amenazas cibernéticas tradicionales, como hackear una computadora portátil a través de Internet y las operaciones de guerra electrónica usuales, como los dispositivos explosivos improvisados radio-controlados que utilizan el espectro electromagnético, se han desdibujado, permitiendo que los sistemas de guerra electrónica accedan a la secuencia de datos para combatir las amenazas de dicha guerra.

Bárbara Opall-Rome[567], en un artículo llamado *"Russian Influence on Hezbollah Raises Red Flag in Israel"*, comenta un informe escrito en hebreo por Dima Adamsky, llamado *"Russian Involvement in Syria: Strategic Significance and Operational Lessons"*, allí, el autor advierte sobre la influencia rusa con respecto a la información, la guerra cibernética y electrónica y el uso de fuerzas especiales - una combinación de capacidades que puede afectar el equilibrio permanente de la disuasión incluso antes de que Israel y Hezbollah vuelvan a enfrentarse cinéticamente.

Según la autora, Adamsky documenta la incursión rusa en la guerra de la información electrónica en el nivel táctico para interferir, reprimir y sabotear a las fuerzas enemigas y el proceso de toma de decisiones del oponente (en este caso las Fuerzas de Defensa de Israel (FDI)). También cita a expertos rusos que muestran la capacidad de Moscú para explotar el espectro electromagnético en su beneficio en las operaciones cibernéticas defensivas y ofensivas a punto tal de poder interferir la capacidad de las FDI y de llevar a cabo operaciones de vehículos no tripulados interfiriendo el ciclo sensor - lanzador (*sensor-to-shooter strike*).

Para Adamsky, "cuando la guerra electrónica se combina con la cibernética, las capacidades cinéticas y los conocimientos [conceptos operativos rusos,] tiene el potencial de crear, para las IDF "ceguera" 'y "sordera" en ciertas operaciones".

Según Senft[568], la integración del Protocolo de Internet (IP) en una amplia gama de sistemas de comunicaciones permite un *jamming* (interferencia) inteligente, como por ejemplo la integración de capacidades IP en los sistemas que utilizan radio frecuencia (RF) para la comunicación ya que proporciona a los atacantes la capacidad de explotación de los sistemas en redes aisladas.

El mismo autor, citando las fuentes, da tres ejemplos basados en evaluaciones de vulnerabilidad real.

---

567 Opall-Rome, Bárbara, Russian Influence on Hezbollah Raises Red Flag in Israel, November 6, 2016, Disponible en: http://www.defensenews.com/articles/russian-influence-on-hezbollah-raises-red-flag-in-israel

568 Senft, Michael, Convergence of Cyberspace Operations and Electronic Warfare Effects, Jan 4, 2016, Disponible en: http://www.cyberdefensereview.org/2016/01/04/convergence-of-cyberspace-operations-and-electronic-warfare-effects/

En el primer caso, una IP a través de un sistema radio desarrollado para proporcionar conexiones de gran ancho de banda de una plataforma aérea a usuarios en el terreno se deshabilitó mediante bloqueo inteligente. La IP a través de sistema de radio estaba protegida contra los ataques de redes tradicionales a través de un protocolo inalámbrico seguro, pero resultó vulnerable a un *jamming* en una banda de frecuencia en potencias muy bajas, con lo cual, la negación de servicio se atribuyó a un error del sistema en lugar de *jamming*. En el segundo caso, las operaciones cibernéticas ofensivas (OCO) y capacidades de guerra electrónica se sincronizaron en un ataque simulado contra una red de comunicación por satélite (SATCOM). OCO se utilizó para obtener acceso y enumerar la red SATCOM para identificar la estación de tierra, que luego fue interferida forzando al blanco a utilizar métodos de comunicación alternativos, proporcionando así posibles nuevas vías de ataque con sus propias vulnerabilidades.

En el tercer caso, un ataque coordinado de operaciones cibernéticas y guerra electrónica sobre un sensor de redes[569] dañó fuertemente una red de malla[570] y evitó que se recibiesen los datos de los sensores sin que se disparase una alerta de una denegación de servicio o de un *jamming*. Estos ejemplos demuestran el poder de efectos sinérgicos a través de la convergencia de las operaciones cibernéticas y de guerra electrónica, efectos que, convenientemente combinados, aumentan la dificultad de montar una respuesta efectiva en la lucha para identificar la fuente del ataque enemigo.

Debe tenerse en cuenta que esta convergencia de efectos puede llegar a disminuir la capacidad de los comandantes para emplear capacidades ofensivas de guerra electrónica debido a que las operaciones cibernéticas ofensivas seguramente requerirán la aprobación por parte de la estrategia militar. En contraste, el empleo de capacidades de guerra electrónica ofensivas (contra – contra medidas electrónicas) por lo general sólo necesita la aprobación del nivel operacional o táctico. Los comandantes con medios adecuados son capaces de impactar rápidamente la red de comunicaciones de radio de un adversario a través de la interferencia de los links o del uso de armas de energía dirigida para destruir a los transmisores. El uso de operaciones cibernéticas para producir el mismo efecto de negarle al enemigo el uso de la red de comunicaciones de radio seguramente requerirá de una cuidadosa planificación, de apoyo de inteligencia y coordinación interagencial, además de la aprobación.

También, existen otras técnicas que utilizan las operaciones ciberelectromagnéticas. La guerra electrónica puede, además, ser llevada a cabo mediante el control de dispositivos que emiten energía de radiofrecuencia y que están presentes en hogares y ciudades: Bluetooth, Wi-Fi, 5G, sistemas de entrada sin llave y sistema global de posicionamiento (GPS), para nombrar algunos.

---

569 El sensor de red se conecta a Internet, una empresa WAN o LAN o a una red industrial especializada para que los datos recogidos puedan ser transmitidos a sistemas terminales para el análisis y utilizados en aplicaciones.

570 Una red de malla es una red área local (LAN), una red de área local inalámbrica (WLAN) o LAN virtual (VLAN) que emplea a uno de los dos arreglos de conexión descentralizada.

Kim Zetter[571] señala que investigadores en Israel han ideado un nuevo método para robar datos que pasa por alto ciertas protecciones como por ejemplo no permitir la utilización de dispositivos USB o aislar a las computadoras de Internet (*air-gapping computers*). Para ello, utilizan la red GSM[572], ondas electromagnéticas y un teléfono móvil elemental. El ataque requiere que tanto el computador de destino como el teléfono móvil tengan instalado un mismo malware de manera tal que el ataque pueda explotar las capacidades naturales de cada dispositivo para extraer los datos. Las computadoras, por ejemplo, emiten radiación electromagnética de manera natural durante su operación normal, y los teléfonos celulares por su naturaleza son *"ágiles receptores"* de esas señales. Estos dos factores combinados crean una *"invitación para los atacantes que buscan extraer datos sobre un canal encubierto"*.

El ataque comprende las señales de radio generadas por la tarjeta de video de una computadora que luego son captadas por el receptor de radio FM en un Smartphone. Funciona con teléfonos celulares simples que normalmente se permiten en entornos en los que los Smartphone no lo son, debido a que solo tienen voz y capacidades de mensajería de texto y probablemente porque no se pueden transformar en dispositivos de escucha. Los investigadores israelíes desarrollaron un *malware* llamado GSMem[573] que fuerza la memoria de la computadora a actuar como una antena y transmitir datos de forma inalámbrica a un teléfono sobre frecuencias de celulares. El malware consume sólo 4 kilobytes de la memoria cuando está en funcionamiento, lo que lo hace difícil de detectar.

El mismo Zetter[574] describe otra modalidad para robar datos de una computadora utilizando el sonido de sus ventiladores.

Aunque la técnica puede utilizarse para robar una cantidad limitada de datos, es suficiente para extraer las claves de cifrado y las listas de nombres de usuario y contraseñas, así como pequeñas cantidades de historias *keylogging*[575] y documentos, desde una distancia de 3 metros. Los investigadores, que han descrito los detalles técnicos del ataque en un documento denominado *Fansmitter: Acoustic Data Exfil-*

---

571 Zetter, Kim, Researchers Hack Air-Gapped Computer with Simple Cell Phone, 07.27.15. 07.27.15, Disponible en: https://www.wired.com/2015/07/researchers-hack-air-gapped-computer-simple-cell-phone/

572 El sistema global para las comunicaciones móviles (del inglés Global System for Mobile communications, GSM, es un sistema estándar, libre de regalías, de telefonía móvil digital. Un cliente GSM puede conectarse a través de su teléfono con su computador y enviar y recibir mensajes por correo electrónico, faxes, navegar por Internet, acceder con seguridad a la red informática de una compañía (red local/Intranet), así como utilizar otras funciones digitales de transmisión de datos, incluyendo el servicio de mensajes cortos (SMS) o mensajes de texto. GSM se considera, por su velocidad de transmisión y otras características, un estándar de segunda generación (2G).

573 El malware GSMem puede ser instalado en un equipo mediante el acceso físico o a través de métodos de interdicción, es decir, en la cadena de suministro, o sea, en la ruta del vendedor al comprador. También puede instalarse a través de ingeniería social, una aplicación maliciosa o acceso físico al teléfono de destino.

574 Zeter, Kim. Clever Attack Uses the Sound of a Computer's Fan to Steal Data. WIRED Disponible en: https://www.wired.com/2016/06/clever-attack-uses-sound-computers-fan-steal-data/

575 Key logger es un tipo de software o un dispositivo hardware específico que se encarga de registrar las pulsaciones que se realizan en el teclado, para posteriormente memorizarlas en un fichero o enviarlas a través de Internet. Suele usarse como malware del tipo daemon, permitiendo que otros usuarios tengan acceso a contraseñas importantes, como los números de una tarjeta de crédito, u otro tipo de información privada que se quiera obtener.

tration from (Speakerless) Air-Gapped Computers, hasta ahora han sido capaces de extraer las claves de cifrado y las contraseñas a un ritmo de 15 a 20 bits por minuto, más de 1.200 bits por hora, pero están trabajando en métodos para acelerar la extracción de datos.

Durante la operación, los ventiladores generan un ruido conocido como *Blade Pass Frequency Noise* que varía en intensidad en función del número de paletas del ventilador y la velocidad de rotación. El ataque consiste en incrementar la velocidad o frecuencia de uno o más de los ventiladores de la computadora para transmitir los dígitos de la clave de cifrado o la contraseña a un Smartphone o a una computadora cercanos, con diferentes velocidades que representan los unos y ceros de los datos que quieren extraer los atacantes— para la prueba, los investigadores utilizaron 1.000 RPM para representar el 1 y 1.600 RPM para el 0.

Para recibir las señales de audio emitidas por la máquina de destino, un atacante necesitaría infectar el teléfono inteligente de alguien que trabaja cerca de la máquina usando un *malware* diseñado para detectar y decodificar las señales de audio que son transmitidas y luego enviadas al atacante vía SMS, transferencia de datos móviles o Wi-Fi. El receptor tiene que encontrarse dentro de ocho metros de la máquina objetivo, por lo que en ambientes donde los trabajadores no pueden llevar sus teléfonos inteligentes, un atacante en su lugar podría infectar una máquina conectada a Internet que se encuentra cerca de la máquina objetivo.

En síntesis. Como se ha podido apreciar existen numerosas formas mediante las cuales las operaciones cibernéticas en apoyo de las operaciones de información pueden ser incorporadas al planeamiento. Para ello, será necesario disponer de una sólida información de inteligencia para saber, entre otras cosas, con la mayor exactitud posible qué medidas de protección de frecuencia utiliza el oponente; si el *spoofig* será exitoso o será detectado a través de algunos engaños; o ¿cuán bien disimula, se oculta o utiliza técnicas de negación y engaño el adversario?

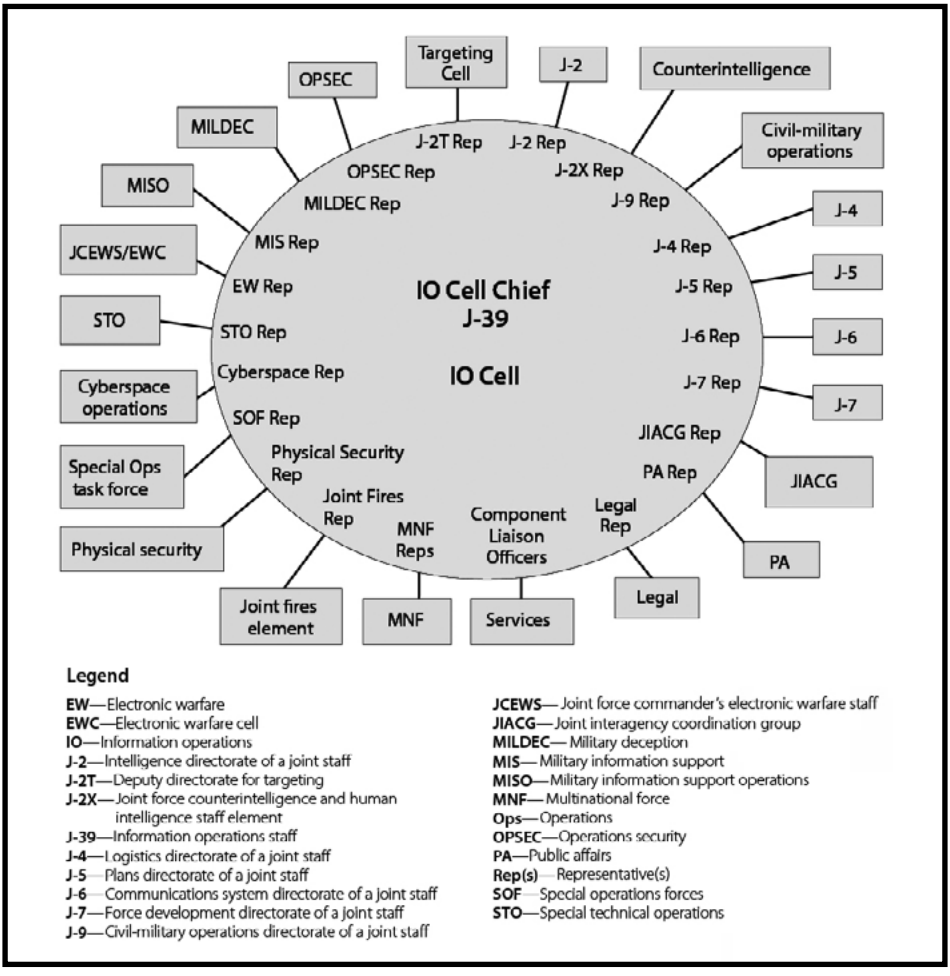
La organización de un Estado Mayor para las operaciones de información

Para lograr esta integración, en los Estados Mayores actuales se establecen células específicas que reúnen a representantes de una amplia variedad de organizaciones como lo muestra la figura 17[576]. Otros proponen la creación, dentro del Estado Mayor del Comandante de Teatro, de un Centro Coordinación de Guerra ciberelectrónica (CEWCC) para dotar al comandante de una herramienta que optimice las operaciones incrementando el tempo y desarrollando ventajas militares[577].

576 Joint Publication JP 3-13; Information Operations; 27 November2012; Incorporating Change 1; 20 November2014; P. II-6 Disponible en: http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf.

577 Maj Matthew E. Poole & LtCol Jason C. Schuette; "Cyber Electronic Warfare: Closing the operational seams"; Marine Corps Gazette; August 2015; Volume 99, Issue 8; Disponible en https://www.mca-marines.org/gazette/2015/08/cyber-electronic-warfare#sthash.d2gPXDVS.dpuf

FIGURA 17: CÉLULA TEÓRICA DE OPERACIONES DE INFORMACIÓN[578]



También, suelen conformarse las denominadas "cibercélulas"[579] las cuales se podrían definir como una capacidad de alta especialización funcional y naturaleza dual –tanto defensiva como ofensiva– con la función de ejecutar una tarea encomendada para garantizar la seguridad y la defensa de un determinado ámbito cibernético. Dependien-

578 JP 3-13 Information Operations Página II-6 Figure II-3. Notional Information Operations Cell.

579 Real Instituto Elcano, Thiber, Las cibercélulas: una capacidad para la ciberseguridad y la ciberdefensa nacionales; ARI 26/2013 - 4/7/2013 Disponible en: http://www.realinstitutoelcano.org/wps/portal/rielcano/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_es/zonas_es/ari26-2013-thiber-cibercelulas-ciberseguridad-ciberdefensa-nacionales.

do de las necesidades operativas y del ámbito en el que ésta actúe, una cibercélula puede tener asignadas tres grandes funciones:

- Ejecutar operaciones cibernéticas específicas o conjuntas con el resto de las dimensiones operativas (terrestre, naval, aérea y espacial).
- Apoyar la evaluación y mejorar el nivel de madurez, resiliencia y seguridad de las capacidades cibernéticas nacionales, aliadas y multinacionales.
- Contribuir a la experimentación de nuevos conceptos operativos y capacidades cibernéticas.

El Mando y Control de las cibercélulas deberá ejercerse en los niveles estratégico, operacional y táctico y cada uno de estos niveles tendrá asignadas un conjunto de responsabilidades y acciones con el propósito de que las cibercélulas desempeñen su tarea con garantías. En el nivel estratégico se definirán los objetivos de alto nivel, las prioridades y los hitos que deben ser alcanzados por la cibercélula durante la tarea encomendada. Además, desde este nivel se deberá garantizar la viabilidad y evolución de la cibercélula, dotándola de todos los recursos humanos, económicos y tecnológicos necesarios. En el nivel operacional, se autorizarán y dirigirán todas las actuaciones pertenecientes a la tarea encomendada y cada una estará controlada por un equipo operativo (EO), de modo que durante la ejecución de una tarea habrá tantos equipos operativos como actividades que forman parte de cada tarea. Asimismo, la composición de estos equipos vendrá determinada por la naturaleza de la tarea. Por último, y en el nivel táctico, los responsables de cada equipo operativo (EO) definirán los planes tácticos de las actividades. Para ello, desglosarán hasta el nivel más granular de definición posible cada una de las acciones que conforman una actividad con el asesoramiento de los responsables de los equipos tácticos asignados a cada acción (cada equipo operativo estará apoyado por tantos equipos tácticos como acciones formen parte de la actividad).

Otra forma de organización es aquella que separa las funciones técnicas de las psicológicas. Tal división implica que las operaciones de red de computadoras se fusionan con las de guerra electrónica y se establecen las áreas de personal para que las apoyen y que los asuntos públicos y las operaciones de apoyo de información militar (antes llamadas operaciones psicológicas) se agrupen en otra área. El producir tal separación de manera artificial: lo psicológico, que se centra en el contenido de los mensajes y personas, y lo técnico, que se ajusta en la entrega de contenido y computadoras, normalmente dificulta la integración que dichos esfuerzos requieren para poder coordinarse de manera eficaz.

Conclusiones del capítulo

En este capítulo se ha podido apreciar cómo, a través del desarrollo de la tecnología de la información y las comunicaciones, ha crecido el rol de la guerra basada en la información en las operaciones militares. El campo de batalla de la información es un ambiente que comprende tres dimensiones: la física, la informativa y la cognitiva, que se entrelazan dentro del ciclo de toma de decisiones.

Con la aparición de la información como un terreno clave en la guerra moderna, la comprensión de su entorno – cómo es enviada y recibida, cómo se percibe, y cómo se

actúa sobre ella – pasó a ser una parte integral de la guerra contemporánea. En este capítulo se ha podido ver cómo las operaciones de información se utilizan para informar, persuadir e influir en la toma de decisiones.

Los conflictos actuales manipulan la información como la fuerza, en lugar de medios físicos, para obligar a actuar a los adversarios y a quienes deben tomar decisiones.

Mientras que las fuerzas de ISIS esparcidas a través de Iraq y Siria, reclamando por pueblos, ciudades, recursos petrolíferos y franjas de tierra, sus sofisticadas campañas en los medios sociales a través del mundo buscan invitar a los corazones y a las mentes de los musulmanes afines, a unirse a su lucha y a colaborar con recursos materiales y económicos.

Videos muy bien elaborados en YouTube, revistas de calidad profesional, campañas en Facebook y Twitter y un orquestado uso de otras plataformas de medios sociales son utilizados con un grado de sofisticación tal que podrían llegar a competir con muchas empresas de Estados Unidos. Radicalización, reclutamiento, formación, miedo y recaudación de fondos son los titulares de sus objetivos y el mundo su mercado.

Para que este tipo de operaciones sean eficaces tienen que tener amplia difusión, ser aceptadas como legítimas e internalizadas por la audiencia. En el caso de la campaña de influencia de Rusia sobre las elecciones estadounidenses de noviembre de 2016, primero los autores debieron ganar la suficiente credibilidad para ser recogidos por medios de Estados Unidos, razón por la cual, WikiLeaks fue utilizado para diseminarla. La inteligencia militar y nacional rusa, supuestamente utilizó un hacker solitario (Guccifer 2.0)[580] para filtrar información gubernamental robada a una ONG real (WikiLeaks) la cual la diseminó al público.

No existiendo una publicación que las defina todavía en el ámbito nacional, para esta obra se adopta como definición de operaciones de información[581] "aquellas que implican el uso y manejo de la tecnología de la información y la comunicación para acceder, modificar, interrumpir, alterar o destruir la información del oponente en procura de obtener una ventaja competitiva, así como asegurar la integridad de la información propia".

En la última década, varias capacidades relacionadas con la información han crecido en el mundo, lo cual revela el valor que se les asigna. Las operaciones de información no están definidas en la doctrina argentina, y es una necesidad hacerlo con premura. La causa de la indefinición es la confusión de operaciones de información con la acción psicológica sobre la propia población, lo que es un concepto ideológico tremendamente errado.

580 El Guccifer original se encuentra preso en una cárcel de EE. UU

581 de Vergara Evergisto. Las operaciones de Información, Instituto de Estudios Estratégicos de Buenos Aires (IEEBA) Disponible en http://www.IEEBA.com.

CONCLUSIONES GENERALES

Los estudiosos de la historia militar dicen que la pólvora, descubierta en China en el siglo IX y utilizada con propósitos militares con el desarrollo de la artillería en el siglo XIII, transformó el campo de batalla, pero la invención y desarrollo del avión ha transformado la propia guerra, causando un enorme efecto tanto en los combatientes como en la población civil, al dejar de ser la guerra un problema de los ejércitos en el campo de batalla para transformarse en un problema de toda la sociedad.

La guerra había dejado de ser un asunto exclusivo de los ejércitos o las marinas, para hacer sentir su influencia más allá del alcance de las armas de fuego. A partir del surgimiento de la tercera dimensión del conflicto, no hay territorio donde la vida pueda trascurrir en completa seguridad y tranquilidad; toda la nación está expuesta al ataque aéreo y el campo de batalla solo será circunscripto por los límites de los países en lucha.

Inevitablemente esta posibilidad de convertir a la nación en el campo de batalla, provocó un cambio profundo en la forma de hacer la guerra, porque las características esenciales que poseía resultaron alteradas radicalmente. Se produjo lo que hoy llamamos un cambio de paradigma, que, si bien no dejó de lado la batalla y la destrucción de los ejércitos enemigos, llevó las hostilidades a la destrucción de la capacidad económica de una nación, la guerra total, donde el desgaste se produce a todas las capacidades del oponente.

Este concepto de guerra total es puramente económico y no debe ser confundido con el concepto político de la guerra total de Ludendorff, en el que se promueve una guerra libre de cualquier restricción política o una subordinación de la política a lo militar cuando la nación está en guerra. O el concepto de guerra absoluta de Clausewitz que es filosófico y que en lo político consideraba la subordinación incondicional de la guerra a la política, pues sin ella no tiene sentido.

La idea de la guerra total también es propia de la guerra asimétrica, en la que la "abismal" diferencia en cantidad y calidad de los recursos militares comprometidos obligan a los bandos a utilizar tácticas atípicas que conforman un paradigma distinto de la guerra de destrucción. En este ámbito, las acciones se producen en todo el territorio y sobre cualquier objetivo rentable, no existe un frente determinado, ni acciones militares convencionales; por el contrario, se basa en una combinación de acciones políticas y militares, implicación de la población civil y otras operaciones similares.

Lo mismo ocurre con lo que hoy se denomina guerra cibernética, que es un modo de conflicto social más débil que las guerras militares tradicionales, en la cual los protago-

nistas, los actores o nodos, usan formas de organización en red y doctrinas, estrategias y tecnologías relacionadas con la era de la información, como, por ejemplo, los teléfonos móviles, emails, sitios web, videoconferencias y redes sociales.

La forma de actuar en esta guerra es multifacética y difícilmente encasillable en los parámetros tradicionales. No se sabe muy bien cuándo están atacando o si se están defendiendo, suelen ser transfronterizas, multi jurisdiccionales, actúan de forma pública y privada, pueden actuar de forma civil y militar, de forma legal e ilegal. Esto hace difícil o incluso imposible para los países hacerles frente asignándole el trabajo a una sola organización estatal para que se haga cargo del problema, como por ejemplo las fuerzas militares, policiales o servicios de inteligencia.

La asimetría en capacidad militar ha pasado a un segundo plano; ahora solamente es suficiente un software, que no requiere de más de unas decenas de líneas de código y un equipo limitado de personas para infringir importantes daños. Como en todo tipo de guerra, la incertidumbre de lo que el enemigo puede llegar a hacer, la niebla de la guerra de Clausewitz, están presentes, aunque en una versión moderna.

Como puede verse, desde la era industrial a la era informática, la difusión de las tecnologías de información ha tendido a cambiar algunos parámetros operacionales, y no siempre en beneficio de quien las posee. Eso ha afectado especialmente la forma de hacer la guerra y dio paso a la denominada guerra híbrida. La infraestructura del espacio cibernético fue desarrollada, pero ahora está abierta y disponible para cualquiera que tenga los medios para acceder a él. Sus consecuencias inmediatas no son letales, por lo tanto, el riesgo de escalar el conflicto es escaso. No obstante, el uso del espacio cibernético puede causar efectos en los niveles táctico, operacional y estratégico, cuando ataca a sistemas de comando y control, no solamente militares sino de instalaciones civiles como usinas eléctricas o cualquier otra fuente de poder hidroeléctrico o nuclear o se pretende alterar los datos de una elección a nivel nacional. Entender las implicancias de emplear capacidades del espacio cibernético en cada uno de esos niveles exige de un estudio particular.

Comprender los efectos de un ataque cibernético es más difícil que el de un ataque con bombas. La precisión tecnológica ha llegado a un momento tal que puede anticiparse, daños, bajas, destrucción y daño colateral para determinados sistemas de armas. Pero con armas cibernéticas es mucho más difícil precisar efectos deseados y separarlos de efectos no deseados. Todo el uso de ciberarmas es complicado por su imprevisibilidad inherente, que arroja dudas sobre la precisión del arma y el efecto. Una vez lanzada, su curso puede ser difícil de predecir y de contener.

La reacción del enemigo es mucho más difícil de predecir, al provenir de efectos que no se pueden controlar. El espacio cibernético es complejo, así que imaginar los efectos de un ataque cibernético que puede ocasionar pánico y urgencias puede generar reacciones inesperadas en el proceso de toma de decisiones enemigo. Por definición, un proceso irracional es difícil de anticipar y los ataques cibernéticos pueden generar respuestas irracionales de los líderes más racionales.

La naturaleza de los conflictos en el espacio cibernético será diferente en función de los objetivos de los participantes. Los criminales buscarán ingresos ilegales, tratando

de apropiarse de partes del espacio cibernético y prosperarán los proveedores ilegales de software malicioso (*malware*). Los servicios de inteligencia intentarán obtener información útil, atacando determinados sectores del espacio cibernético, sean estos enemigos, amigos o neutrales, para obtener acceso a esa información. Los militares procurarán interrumpir las operaciones del enemigo, por lo que atacarán sus sensores, su logística, sus sistemas de comunicaciones y de control en el espacio cibernético enemigo. Los conflictos podrán ser tan simples como disputas civiles respecto de la propiedad del nombre de un dominio o tan complejos como campañas de ataque cibernético deliberado como parte de una guerra convencional entre países.

La guerra cibernética se puede resumir en tres puntos. Implica acciones que logran un efecto político o militar, entraña el uso del espacio cibernético para proporcionar efectos cinéticos directos o en cascada que tienen resultados comparables a las capacidades militares tradicionales y crea resultados que causan o son un componente crucial de una seria amenaza a la seguridad de la nación o que se llevan a cabo en respuesta a tal amenaza. Sus efectos más importantes probablemente serán la negación o manipulación de las capacidades de comando militar, control, comunicaciones, computadoras, inteligencia, vigilancia y reconocimiento (C4ISR) y la degradación de las redes de apoyo civil.

El espacio cibernético, por su parte, es un entorno basado en estructuras de red que privilegia la accesibilidad por sobre la seguridad y existen considerables dificultades técnicas y jurídicas para atribuir con precisión los ataques cibernéticos y poder tomar algún tipo de represalia, pero fabricar un arma cibernética, ultra secreta como Stuxnet, requiere poseer una tecnología adecuada, recursos humanos y materiales para probarla, hacer inteligencia sobre el objetivo y entregarla, lo cual hace presumir que el costo no solo yace en la creación.

Para la República Argentina, sigue siendo de carácter transversal a los ambientes operacionales terrestre, naval y aéreo. Sin embargo, la Organización del Tratado del Atlántico Norte acaba de reconocer oficialmente, en junio de 2016, al espacio cibernético como un ambiente operacional que se suma a los tradicionales de aire, mar y tierra lo cual significa que, los ataques llevados a cabo de esa manera pueden desencadenar una respuesta del artículo 5, que es una acción colectiva de la organización de 28 miembros contra el autor de un incidente de espacio cibernético encaminada a cualquier estado protegido por la OTAN. Antes, sólo las acciones que se llevaban a cabo en las zonas tradicionales, tierra, mar o aire, tenían ese potencial.

Por ello, la capacidad de contar con un arma cibernética la puede poseer cualquier Estado o persona que tenga la experiencia y los recursos necesarios, pero el peligro aparece cuando ese Estado o esa persona está dispuesta a ofrecerla y/o "arrojarla". Por lo tanto, es la intención poseer las habilidades necesarias para desarrollar y desplegar las ciberarmas, lo que debe ser uno de los objetivos de cualquier estrategia de seguridad y defensa nacional que involucre a la guerra cibernética.

Hasta el presente no existen definiciones universalmente consensuadas en lo que respecta a los términos relacionados con la ciberdefensa y la ciberseguridad aunque haya una de guerra cibernética de la Organización de las Naciones Unidas y otra de ciberseguridad en la Unión Internacional de Telecomunicaciones.

La forma de atacar de los agresores en el espacio cibernético junto con el anonimato de los atacantes también juega su rol importante. Inicialmente pueden detectarse intentos de intrusión, pero no puede atribuirse su propósito. Puede tratarse de un adolescente, de una pandilla de criminales cibernéticos, de un ataque a los sistemas de defensa, de espionaje comercial, de ataques a infraestructura crítica, o industrial, o de fraude financiero.

El auge del mundo interconectado también ha generado considerables retos, que socavan estos beneficios y representan una seria amenaza al potencial del mundo cibernético. Curiosamente, afecta a los más desarrollados en el tema, y mucho menos a los menos desarrollados. Así, estos últimos han encontrado un arma barata para dañar a los más poderosos. Cuanto más un Estado desarrolle sus transacciones económicas a través de Internet, cuanto mayor sea la cantidad de usuarios de la telefonía móvil y la tasa de uso de Internet, más vulnerable será y más deberá considerar el desarrollo de sistemas gubernamentales y militares que de manera eficiente y eficaz sean capaces de producir las adecuadas contramedidas.

Por otra parte, cuanto más ciberdependiente sea un Estado, más se cuidarán sus posibles agresores de atacarlo, por temor a una represalia, lo que no significa que pueda disuadir a todos aquellos, que simplemente desean obtener información clasificada.

Frente a esta realidad, los Estados tratan de acordar una definición respecto de lo qué puede ser considerado como un ataque y cuál debiera ser una respuesta proporcional. Para resolver este y otros dilemas, es necesario de la cooperación internacional para establecer nuevas normas, pero mientras se trata de lograrlo, se preparan para auto defenderse de manera unilateral, de una amplia gama de ataques que se extiende desde aquellos que pueden ser ejecutados por actores extranjeros cuasi – estatales hasta robos perpetrados por delincuentes nacionales.

Si bien la mayoría de los países adhiere a la teoría de que para ser definida como "agresión" debe llegar a provocar algún daño material o personal, no hay un consenso generalizado, lo cual lleva a que quien posea capacidades como para hacerlo, responda a un ataque por medios cinéticos o no cinéticos aun cuando las normas del Derecho Internacional actual no llegan a regular de forma efectiva las nuevas amenazas que emergen del espacio cibernético. El Manual Tallin 2.0 es útil en el derecho internacional aplicable a las operaciones cibernéticas, pero no establece ninguna nueva ley internacional ni representa la *opinio juris* de ningún Estado con respecto a las acciones que tomen o puedan tomar en el ciberespacio.

En cuanto a las operaciones cibernéticas, de lo investigado surge que ellas pueden clasificarse en ofensivas, defensivas (activas y pasivas) y de exploración y que, quien se prepara para defenderse, debe conocer, además de sus vulnerabilidades, cómo se ejecutan los ataques, con lo cual, ya sabe hacerlos. Para poder ejecutarlas es necesario poseer una serie de capacidades que comprenden las de detección, de análisis de flujo de redes, de ingeniería reversa, de respuesta y otras que ya se han mencionado en esta investigación. Tanto las estrategias de ciberseguridad como el Manual Tallin 2.0 dejan claro que la defensa activa y la ofensiva cibernética solamente las ejecutan los Estados.

No existe un Derecho Internacional que incluya la guerra cibernética. El Manual Tallin, escrito por un grupo de expertos de todo el mundo, pese a que no tiene ninguna si-

tuación legal y no representa la opinión de la OTAN por sí, puesto que la interpretación y aplicación de las normas del manual son discutibles, se ha convertido en un recurso importante para los asesores legales respecto de las cuestiones cibernéticas.

En la presente obra no se han analizado delitos cometidos a través de Internet y otras redes informáticas, relacionados con los derechos de autor, el fraude informático, la pornografía infantil, los delitos de odio y violaciones de seguridad de red contemplados en el Convenio sobre ciberdelincuencia, también conocido como el Convenio de Budapest pero debe quedar claro que pese a la diferencia entre la ciberseguridad y la ciberdefensa y entre estas y la seguridad informática, las agendas deben integrarse y no separarse.

Sí se ha tratado de explicar que la protección de las infraestructuras críticas de un país, tanto civiles como militares, deben ser defendidas por un conjunto de esfuerzos que no son solo competencia de las fuerzas de seguridad, sino también de las fuerzas armadas, de las empresas y de los individuos, pues ello hace a la seguridad y la defensa nacional. La potenciación de la resiliencia debe ser una tarea ineludible, ya que se debe ser capaz de minimizar los efectos provocados por los ciberataques y recuperar lo antes posible la capacidad de operar.

Sin embargo, para ello se hace necesario contar con una Política o Estrategia Nacional de Defensa Cibernética, derivada de una Estrategia Nacional de Seguridad Cibernética resultante, a su vez, de una Estrategia Nacional de Seguridad y Defensa Nacional pues, cada una refuerza las razones de la otra. En el caso de las dos últimas, no debe olvidarse que una agresión militar convencional podría venir acompañada -en el antes, durante o el después - de un ciberataque. Y al revés: un ciberataque militar podría venir acompañado de acciones más convencionales. Como se ha visto, los países están creando unidades militares preparadas para la guerra cibernética, pero ¿solo para detectar, detener o mitigar ataques?, ¿o también con capacidad para, por ejemplo, plantar con antelación suficientes bombas lógicas en las infraestructuras críticas, civiles o militares, de un adversario potencial y activarlas cuando sea necesario?

A partir de un análisis de riesgo de un ataque cibernético, la Estrategia Nacional de Seguridad Cibernética deberá contribuir con la Política de Seguridad y Defensa Nacional fomentando la formación y capacitación, el desarrollo de la tecnología, el conocimiento de la situación cibernética, la coordinación eficiente de los esfuerzos de los diferentes ministerios y organismos públicos para evitar la duplicación de funciones, las ejercitaciones tanto en el nivel nacional como internacional y la colaboración público-privada, todo ello, a través de una legislación y una financiación adecuadas.

Por su parte, la Política o Estrategia Nacional de Defensa Cibernética deberá definir objetivos, líneas de acción, cronogramas de trabajo y pautas para la organización de las unidades de Defensa Cibernéticas que resulten necesarias en el contexto de los objetivos fijados por la Política de Seguridad y Defensa Nacional.

La finalidad última de ellas debe ser la protección activa y pasiva de los activos nacionales teniendo presente que las indefiniciones estratégicas pueden conducir a indefiniciones operacionales, con implicancias quizás de relevancia en términos económicos y en términos de derechos básicos. El hecho de que mediante el decreto 577/2017 se conformara un organismo para generar una estrategia de ciberseguridad es un paso importante.

El conjunto de políticas y estrategias así elaboradas permitirá redactar una Doctrina Militar de Ciberdefensa que proporcione unidad de pensamiento en el ámbito del Ministerio de Defensa y contribuya a mejorar el accionar militar conjunto de las Fuerzas Armadas en el espacio cibernético.

Simultáneamente con lo expresado hasta el momento, en la investigación también se ha demostrado que se asiste a lo que ha dado en llamarse guerra híbrida, entendiendo como tal, la que emplea una combinación de operaciones convencionales y asimétricas, operaciones de información y de guerra cibernética. Es una nueva modalidad de hacer la guerra, podría decirse "del débil al fuerte".

Hasta el año 2015, las fuerzas armadas argentinas tenían vedadas las operaciones de información debido a restricciones político-ideológicas; de aquí que la propia doctrina no ha tenido en cuenta estas tendencias, lo cual lleva a imponer límites artificiales que obstaculizan la implementación de las operaciones de información y de ciberdefensa. Además, el personal que en alguna eventualidad debería planificarlas, no es siempre bien comprendido, lo cual implica que su eventual ejecución no podría llegar a ser tan efectiva como debería ser.

Por lo que se ha mostrado a lo largo de esta obra, estas operaciones destinadas a confundir a un oponente en su proceso de toma de decisiones, a la vez que proteger los propios sistemas, merecen publicaciones doctrinarias similares a las de todos los otros países; razón por la cual, resulta imperioso elaborar una publicación conjunta sobre las operaciones de información, que son las operaciones donde ejercen su influencia las operaciones cibernéticas.

Asimismo, se considera que debe definirse la doctrina de las operaciones de información y de las operaciones cibernéticas, reorganizar el sistema e instruir y adiestrar al personal a fin de adaptarse a las nuevas tendencias. Una forma de implementar esto último sería la de incorporar a los programas de educación militar conjuntos las operaciones cibernéticas y, por ende, las de información, que deberían contemplar la forma de integrar las operaciones ciberespaciales en la planificación conjunta de nivel estratégico y operacional y sus capacidades y limitaciones.

De igual manera que hubo que desarrollar la teoría del poder aéreo y ajustar la teoría global del conflicto, se necesita una teoría para las operaciones en el espacio cibernético que permita entender las implicancias de usar las capacidades del espacio cibernético en los niveles estratégico, operacional y táctico.

Para ello, es importante comprender la relación existente entre las operaciones cibernéticas y las de información. Las primeras se vinculan con el uso de las capacidades del espacio cibernético para crear efectos en apoyo de las operaciones a través de los dominios físicos y el espacio cibernético. Las de información, a pesar de que también utilizan las capacidades de los dominios físicos para lograr sus objetivos, se vinculan más específicamente con el empleo integrado de las capacidades relacionadas con la información durante las operaciones militares, en concierto con otras líneas de operación para influir, alterar, corromper o usurpar la toma de decisiones de adversarios y potenciales adversarios; al mismo tiempo que se protegen los propios. Así, el espacio cibernético es un medio a través del cual algunas capacidades relacionadas con la información, como

la información militar en apoyo de las operaciones (MISO – ex Operaciones psicológicas) o el engaño militar (MILDEC), pueden ser empleados.

Mientras que algunas operaciones cibernéticas pueden apoyar objetivos de las operaciones de información, otras se ejecutarán en apoyo de objetivos específicos o para apoyar operaciones en los dominios físicos como, por ejemplo, el ataque físico con sistemas de armas cibernéticas como el uso de drones, y el ataque por red informática.

Por su parte, las operaciones de información no se reducen a ser una herramienta de las operaciones cibernéticas, sino que también abarcan la guerra electrónica, las operaciones antiguamente llamadas psicológicas, las operaciones de seguridad y el engaño militar, entre otras. Las operaciones en el ciberespacio pueden apoyar directamente a las operaciones de información y estas, aun cuando no sean cibernéticas, pueden afectar a las operaciones del ciberespacio.

Para poder cumplir con estas particularidades, las autoridades del espacio cibernético que se establezcan en el nivel de la estrategia militar deben preparar y establecer el mejor alcance factible tanto virtual como físico y humano, un conocimiento compartido de gestión del espacio cibernético en las tres Fuerzas Armadas y la capacidad de identificar, crear y explotar efectos cibernéticos.

Tras lo dicho, lógico sería entonces que el Comando Conjunto de Ciberdefensa coordinara sus acciones con el Comandante del Teatro de Operaciones, los centros de ciberdefensa de cada una de las Fuerzas Armadas, estableciera los criterios rectores del nivel estratégico militar para la determinación de infraestructuras críticas a ser protegidas, tuviera responsabilidad primaria en medidas de seguridad de la información y la seguridad cibernética y, según se lo ordenen, llevar a cabo determinadas operaciones cibernéticas de proyección de poder cibernético en el espacio cibernético.

En cuanto al Comandante del Teatro de Operaciones, durante el planeamiento y la ejecución de la campaña, deberá articular la forma para que las ciberoperaciones contribuyan a cada fase de la operación, sincronizarlas en cada una de ellas y determinar cómo los objetivos y efectos cibernéticos le permitirán o facilitarán el logro del estado final deseado.

Las operaciones cibernéticas no son planificadas desde que se decide el empleo de las Fuerzas Armadas, sino que se inician desde que se anticipa la contingencia en el planeamiento de la estrategia militar.

Dentro del nivel operacional de implementación de la decisión política, el componente cibernético del Teatro de Operaciones debería, además de cumplir con las funciones administrativas[582], estar en condiciones de poder conducir aquellas operaciones de información, operaciones basadas en redes y de inteligencia que empleen instrumentos cibernéticos.

Históricamente, un Comandante tiene que agrupar hombres y equipos en el campo de batalla para concentrar el poder militar. El uso del espacio cibernético permite que el comandante operacional geográficamente disperse a la fuerza, aunque concentre los esfuerzos de ella sobre el enemigo.

---

582 En las funciones administrativas de la conducción militar, la cibernética tiene amplia participación con elementos burocráticos del S3P, en la logística, en el entrenamiento, en la educación, en la atención médica, en las adquisiciones y administración de personal.

Al mantener a su personal empeñado con el enemigo, pero ubicado fuera del área de combate, un comandante operacional puede influenciar al enemigo sin poner en peligro la seguridad de las propias fuerzas en el espacio cibernético.

Las operaciones de ataque de redes de computadoras complementan a la guerra operacional porque su efectividad se incrementa cuando se integra a otros dominios. De esta forma, los comandantes pueden optimizar los factores de tiempo, fuerza y espacio para lograr objetivos con menor destrucción y menos riesgo de personal.

Si bien la guerra cibernética puede utilizar algunos de los principios de la guerra cinética, hay otros principios que tienen poco o ningún significado en el espacio cibernético.

cibernético consiste en líneas de operaciones, puntos decisivos, centro de gravedad y estado final deseado. Todos los elementos del diseño operacional deben servir para alcanzar el estado final y el plan puede ser ajustado a todos los niveles de la guerra para elaborar más de un centro de gravedad (estratégico militar u operacional) o un estado final (estratégico militar u operacional).

Al tener en cuenta los elementos del diseño y arte operacional del espacio cibernético y del ambiente de la información, los planificadores y los expertos en ciberdefensa llegarán a un punto común donde pueden comprender y contribuir mutuamente, lo cual redundará en un plan de campaña que integre estas operaciones con las convencionales.

Con el incremento del empleo de dispositivos inteligentes, teléfonos, electrodomésticos e incluso autos, cada día las personas se encuentran más interconectadas a través de la tecnología. El creciente uso de redes sociales y otras mejoras como una consecuencia natural de la evolución tecnológica han facilitado la labor de los agentes de inteligencia y los delincuentes cibernéticos. El obtener información a través de una fuente abierta y redes sociales como Facebook, Twitter, LinkedIn, Instagram y otros se ha convertido en una tarea fácil incluso para un simple usuario de Internet, también a través de redes más complejas como TOR.

En este cambiante ambiente de seguridad, las organizaciones militares están revisando la forma de redactar los planes y procedimientos para apoyar la flexibilidad de las operaciones, adaptarse a imprevistos, nuevas amenazas y riesgos a los que tarde o temprano podrán quedar expuestas.

Quien desee profundizar en las razones de estas conclusiones podrá hacerlo en los contenidos de los seis capítulos que abarca esta investigación, que ha llevado más de tres años de discusiones, de intercambios de ideas, de entrevistas, de lecturas en diferentes idiomas y de asistencia a simposios y conferencias.

Con esta obra no se ha pretendido revelar la verdad, simplemente se ha procurado despertar el interés, estimular el pensamiento y estimular los procesos de decisión. Como señalaba Sheldon[583] en 2011, "Es mucho lo que es eminentemente discutible sobre el poder cibernético que sin duda otros tendrán que resolver, pero la creciente comunidad

583 Sheldon, John B., Deciphering Cyberpower Strategic Purpose in Peace and War, Strategic Studies Quarterly, Summer 2011, P. 95. Disponible en: http://chrisherwig.org/data-src/pdf/8876b319-53b5-11e2-9e9b-5c969d8d366f-deciphering-cyberpower-strategic-purpose-in-peace-and-war.pdf

de pensadores debe centrarse en las implicancias estratégicas como cuestión de urgencia para que lo involuntario no se transforme en catástrofe"

La guerra cibernética es nueva, por lo que sus parámetros e implicancias esperan ser descubiertos. Esto significa que sólo una larga discusión y el debate pueden iniciar el proceso de identificación de sus principios más importantes. Cuanto antes empiecen los expertos, mejor.

Reflexiones Finales

En un mundo global y digitalizado, la revolución tecnológica ofrece grandes ventajas, pero también importantes riesgos que deben ser acometidos con eficacia para evitar daños económicos y problemas de seguridad y defensa. Permanentemente ocurren hechos nuevos como el ciberataque global de *ransomware* que afectó, el 12 de mayo de 2017, a empresas privadas y entes estatales de casi un centenar de países. Para ese entonces, esta investigación prácticamente estaba concluida y en proceso de revisión, y si bien este ciberataque podía ser un hecho previsible no parecía plausible.

La Marina de Estados Unidos está examinando si la colisión de un destructor con un barco mercante ocurrida el 21 de agosto se debió a que hackers desconocidos se infiltraron en los sistemas informáticos del USS John S. McCain antes de la colisión.

Estos casos seguramente no serán los último de estas características. Dado el rango de posibles amenazas y el ritmo al que pueden aparecer, se hace imposible preservar todo, en todas partes, todo el tiempo, pero al menos debe ser posible asegurarse de que los recursos más valiosos estén debidamente protegidos.

No puede esperarse que las entidades comerciales y privadas se defiendan en el ciberespacio de los ataques de gobiernos extranjeros o grupos paraestatales pues no tienen la capacidad, la habilidad, ni la autoridad para responder de una manera que sea plenamente eficaz. Tampoco que lo puedan hacer las fuerzas armadas por un lado y las de seguridad y policiales por otro. Si bien el intercambio de información y la colaboración no son un fin, son un medio para alcanzar una mejor defensa nacional cibernética.

La velocidad con que se suceden los hechos hace que los individuos y las organizaciones se vean forzados a tomar decisiones apresuradas y poco eficaces debido, generalmente, a una mayor dependencia en supuestos no probados. Por ello, resulta imperioso contar con mecanismos y herramientas que permitan identificar y afrontar correctamente estos supuestos para mejorar los procesos de toma de decisiones y poder, de forma exitosa, defender, atacar y adaptarse en el campo de batalla cibernético.

Se espera que esta obra sirva para que quienes posean inquietudes con respecto a las operaciones cibernéticas puedan indagar sobre los distintos aspectos que de ella se han tratado, pues las cuantiosas aristas que involucran bien pueden dar lugar a diversas líneas de investigación y, a su vez, al estudio de multiplicidad de temáticas específicas derivadas.

A nuestro entender, fundamentalmente se debería comenzar por analizar cómo el gobierno y el sector privado se relacionarán uno con el otro en el ciberespacio definiendo líneas claras y explicitando ciertas responsabilidades, capacidades y autoridades. Dado que un principio clave del ataque en el ciberespacio es el de hacerlo sobre los sistemas de comando y control, reglas claramente definidas, lo que incluye la identificación

de las áreas donde habrá una superposición de responsabilidades, este ayudará a minimizar las posibilidades de un ataque cibernético. Todo ello tendría que quedar plasmado en una estrategia o política de seguridad y defensa cibernética.

Otra propuesta es tratar de encontrar la manera de aprender a trabajar interagencialmente en un ambiente de cooperación para enfrentar las amenazas a la nación en el espacio cibernético. Al igual que las fuerzas armadas argentinas después del conflicto del Atlántico Sur han aprendido a entrenar, ejercitar, funcionar y operar en un entorno conjunto, también hoy en la República Argentina los sectores público y privado, las universidades, las fuerzas de seguridad y las fuerzas armadas, deberían entrenar, ejercitar y operar de manera cooperativa en el ciberespacio.

A partir de la realización de este trabajo se ha podido entender y reconocer dónde "se está parado" en lo que a ciberseguridad y ciberdefensa se refiere. El propósito más loable es poder sumarse a pensar juntos hacia dónde se quiere ir.

BIBLIOGRAFÍA

Libros

- Applegate, Scott D., *The Principle of Maneuver in Cyber Operations*, 2012 4th International Conference on Cyber Conflict C. Czosseck, R. Ottis, K. Ziolkowski (Eds.) 2012 © NATO CCD COE Publications, Tallinn.
- Aven, T. and O. Renn, *Risk Management and Governance: Concepts, Guidelines and Applications,* Berlin, Springer Verlag, Ed 2010.
- Beaufre André, *Introducción a la estrategia,* Traducción al español de la Editorial Struhart y Cia, Año 1962.
- Flores, Héctor, "Los ámbitos no terrestres en la guerra futura: espacio cibernético". En Flores, H. (comp.) *Los ámbitos no terrestres de la guerra futura: espacio cibernético-aeroespacio,* Estado Mayor Conjunto de las Fuerzas Armadas - Gabinete de Estrategia Militar, Buenos Aires, 2012
- Freedman, Lawrence, *Strategy: A History,* Oxford University Press, Edición 2013.
- Greenberg, Lawrence T. y otros, *Information Warfare and International Law,* National Defense University, Institute for National Strategic Studies, ISBN 1-57906-001-3, Washington DC EEUU, Año 1998.
- Kissinger, Henry, Orden Mundial: *Reflexiones sobre el carácter de las naciones y el curso de la historia,* Penguin Random House Grupo Editorial Buenos Aires, S.A. 2016.
- Kramer, Franklin D., Starr, Stuart H. and Wentz, Larry, *Cyberpower and National Security,* Edited by Center for Technology and National Security Policy, National Defense University Press and Potomac Books, Washington DC, 2009.
- Liang, Q., & Xiangsui, W., *Unrestricted warfare,* Beijing: PLA Literature and Arts Publishing House, 1999.
- McChrystal, Stanley, Gral. US. Army, (Ret.) *Teams of Teams: New Rules of Engagement for a Complex World,* Portfolio/Penguin, 2015.
- Nye, J. and Donahue, J. (edits.), *Governance in a Globalizing World,* Washington, D.C., Brookings Institution, Ed 2000.
- Schmitt, Michael N. General Editor, *Tallinn Manual on the International Law Applicable to Cyber Warfare,* Prepared by the International Group of Experts at the Invitation of The NATO Cooperative Cyber Defence Centre of Excellence.
- Singer, P. W. and Friedman, Allan, *Cybersecurity and Cyberwar What Everyone Needs to Know,* Oxford University Press, Washington DC, Ed. 2014.
- Stel, Enrique, *Guerra Cibernética,* Ed. Círculo Militar, 1ra. Edición, Ed 2005, Buenos Aires, Argentina.

- Sun Tzu, *The Art of War,* traducido por Samuel B. Griffith, Oxford University Express, 1963.
- Thucydides, *History of the Peloponnesian War,* Penguin Classics, Edición 1972.
- Van Creveld, Martin, *Technology and War: From 2000 B.C. to the Present,* Ed. Simon and Schuster, 11 May. 2010.
- Vego, Milan N., *Joint Operational Warfare Theory and Practice.* Newport RI: (Naval War College) Reprint of 1st ed. 2009.
- von Clausewitz, Carl, *On War,* traducido por Michael Howard and Peter Paret, Princeton University Press, 1976.

Revistas

- Bonner, E. Lincoln III, "Cyber Power in 21st Century Joint Warfare", *Joint Force Quarterly 74,* 3rd Quarter 2014.
- Brandes, Sean: "The Newest Warfighting Domain: Cyberspace", *Synesis: A Journal of Science, Technology, Ethics, and Policy,* 2013, Potomac Institute Press.
- Conti, Gregory, and Surdu, John, "Army, Navy, Air Force, and Cyber—Is It Time for a Cyberwarfare Branch of Military?" *IAnewsletter*, Vol. 12, No. 1, Spring 2009.
- Defense Systems Staff, "France moves to boost cyber warfare skills among officer corps", *Defense Systems,* 5 de julio de 2012.
- Duggan, Patrick Michael, "Strategic Development of Special Warfare in Cyberspace", Joint Force Quarterly 79, 4 th Quarter 2015.
- Dombrowski, Peter and Demchak, Chris C., "Cyber War, Cybered Conflict, And The Maritime Domain", *Naval War College Review,* Volume 67, Number 2, 2014.
- Dunlap, Charles J. Jr., Major General, USAF, Retired, "Perspectives for Cyber Strategists on Law for Cyberwar", *Strategic Studies Quarterly. S*pring 2011.
- Eikmeier, Dale C., "Waffles or Pancakes? Operational- versus Tactical-Level War Gaming" *Joint Force Quarterly 78,* 3rd Quarter 2015.
- Fink, Kallie, Capitán de Corbeta, Armada de EUA, Jordan, John D. Mayor, Cuerpo de la Infantería de Marina de EUA, y Wells, James Mayor E., Fuerza Aérea de EUA "Consideraciones para las ciberespaciales ofensivas", *Military Review* en español, mayo-agosto 2014.
- Gjelten, Tom, "Shadow Wars: Debating Cyber Disarmament", *World Affairs,* November / December 2010.
- Gómez Arriagada, Héctor, "Ciberoperaciones", *Revista Marina,* Chile 4 /2013.
- Gómez de Ágreda, Ángel "Integrando lo "Ciber" en las Operaciones", *Revista de Aeronáutica y Astronáutica,* Nº 846.
- Hicks, J. Marcus, A Theater-Level Perspective on Cyber, *Joint Force Quarterly,* 76, 1st Quarter 2015.
- Hughes, Daniel and Colarik, Andrew M., Predicting the Proliferation of Cyber Weapons into Small States, *Joint Force Quarterly 83,* October 01, 2016
- Kanwal, Gurmeet, "China's Emerging Cyber War Doctrine", *Journal of Defence Studies,* Vol 3. No 3. July 2009.
- Libicki, Martin C., "What Is Information Warfare?" *Strategic Forum,* Number 28, May 1995.

- Libicki, Martin C., The Convergence of Information Warfare, *Strategic Studies Quarterly* • Spring 2017.
- López, Claudio C., "La Guerra Informática", *Boletín del Centro Naval,* Número 817, Mayo/agosto de 2007.
- Ortiz, Javier Ulises, "Estrategias de Defensa Cibernética en la Era de la Información". Escuela Superior de Guerra del Ejército Argentino, *La Revista,* Nro. 582. Buenos Aires.
- Poole Matthew E. Maj and Schuette, Jason C. LtCol, "Cyber Electronic Warfare: Closing the operational seams", *Marine Corps Gazette,* August 2015, Volume 99, Issue 8.
- Rexton Kan, Paul, "¿Cómo analizar la guerra en Wi-Fi: de guerra cibernética a Wikiguerra: la lucha por el espacio cibernético?", *Military Review,* septiembre-diciembre 2014.
- Rid, Thomas and Buchanana, Ben, "Attributing Cyber Attacks", *Journal of Strategic Studies,* 23 Dec 2014.
- Poole Matthew E. Maj and Schuette, Jason C. LtCol, "Cyber Electronic Warfare: Closing the operational seams", *Marine Corps Gazette,* August 2015, Volume 99, Issue 8.
- Rexton Kan, Paul, "Cómo analizar la guerra en Wi-Fi De guerra cibernética a Wikiguerra: la lucha por el espacio cibernético" *Military Review,* septiembre-diciembre 2014.
- Sheldon, John B., "Deciphering Cyberpower Strategic Purpose in Peace and War", *Strategic Studies Quarterly,* Summer 2011, P. 95.
- Smith, David J., "Russian Cyber Capabilities, Policy and Practice", *Focus Quarterly,* Winter 2014.
- Umpleby, Stuart A. and Dent, Eric B. "The Origins and Purposes of Several Traditions in Systems Theory and Cybernetics", *Cybernetics and Systems: An International Journal,* 30:79-103, 1999.
- U.S. Cyber Command Combined Action Group, "Beyond the Build: How the Component Commands Support the U.S. Cyber Command Vision", *Joint Forces Quarterly* 80, 1st Quarter 2016.
- Uzal, R., "Ciber Jus ad bellum – ciber jus in bello: Aportes para definir las reglas de empeñamiento militar de Argentina y de otros países de la Región en los casos de Cíber-Conflictos entre estados naciones". *Consejo Argentino para las Relaciones Internacionales* – Boletín Nro 62 (Seguridad y Defensa), noviembre de 2015.
- Williams, Brett T.; "Ten propositions regarding cyberspace operations"; *Joint Force Quarterly* 61; 2º quarter 2011.
- Williams, Brett T., "The Joint Force Comamnder's Guide to Cyberspace Operations", *Joint Forces Quarterly*, 2nd Quarter 2014, Forum.
- Williams, Brett, T "Cyberspace: What is it, where is it and who cares?" A*rmed Forces Journal.* March 13, 2014.
- Zarza, Leonardo Arcadio, "Conducción Militar por Funciones de Combate", *Revista Visión Conjunta*, Año 7 Nro. 13, 2015.

Documentos electrónicos

- Ackerman, Spence, "Darpa Begs Hackers: Secure our Networks," Disponible en *https://www.wired.com/2011/11/darpa-hackers-cybersecurity/*

- Aiken, Klée and Woodall, Jessica, "Tallinn2.0 Cyberspace and the law", Disponible en Internet *http://www.aspistrategist.org.au/tallinn-2-0-cyberspace-and-the-law/*
- Alkhouri, Laith & Kassirer, Alex, "Tech for Jihad", July 2016, Disponible en: *https://www.flashpoint-intel.com/wp-content/uploads/2016/08/TechForJihad.pdf*
- Angerman, William S., "Cyber Power for the Joint Force Commander: An Operational Design Framework". Disponible en *http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA603670*
- Angulo, Martín, Hackearon más de 30 correos oficiales del Ministerio de Seguridad, Disponible en: *http://www.infobae.com/politica/2017/01/31/hackearon-mas-de-30-correos-oficiales-del-ministerio-de-seguridad/*
- Arquilla, John, Ronfeldt, David "In Athena's Camp Preparing for Conflict in the Information Age" Disponible en *http://www.rand.org/pubs/monograph_reports/MR880.html*
- Barbeito, Gabriel, LA CIBERDEFENSA, Universidad de Belgrano, Centro de Estudios para la Defensa Nacional, Boletín N° 22, noviembre de 2016.
- Baker, Prentiss O., Psychological Operations Within the Cyberspace Domain, Disponible en: *www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA519576*
- Bloch, Roberto Dr, "Cibernética", Disponible en *http://uprociber.blogspot.com.ar/2008/04/cibernetica.html*
- Bugorkova, Olga, "Ukraine conflict: Inside Russia's 'Kremlin troll army", 19 marzo 2015 Disponible en *http://www.bbc.com/news/world-europe-31962644*
- Chaparro, Enrique, "El gobierno de Internet", Disponible en *http://www.vialibre.org.ar/2004/08/27/el-gobierno.de-la-Internet*
- Chertoff, Michael and Tobby, Simon The Impact of the Dark Web on Internet Governance and Cyber Security Paper Series: No. 6 — February 2015, Centre for International Governance Innovation and the Royal Institute for International Affairs, Disponible en: *https://www.ourInternet.org/sites/default/files/publications/GCIG_Paper_No6.pdf*
- Clay Wilson, "Information Operations, Electronic Warfare, and Cyberwar: Capabilities and Related Policy Issues", Disponible en *http://www.history.navy.mil/research/library/online-reading-room/title-list-alphabetically/i/information-operations-electronic-warfare-and-cyberwar.html#intro*
- Coffey, Luke Syria's online battlefield; Aljazeera net; 17 junio 2015 Disponible en *http://www.aljazeera.com/indepth/opinion/2015/06/syria-online-battlefield-150617072048625.html.*
- Cohen, Ariel and Hamilton, Robert E. "The Russian Military and the Georgia War: Lessons and Implications" Disponible en *www.strategicstudiesinstitute.army.mil%2fpubs%2fdisplay.cfm%3fpubID%3d1069/RK=0/RS=Cg7zusp5ji3Yfru8gLyYp_1hSVk-*
- Colarik, Andrew and Janczewski, Lech, "Establishing Cyber Warfare Doctrine", Journal of Strategic Security, Volume 5 Issue 1 2012, pp. 31-48. Disponible en: *http://scholarcommons.usf.edu/cgi/viewcontent.cgi?article=1123&context=jss*
- Cortés Ruiz, Pedro, "El Concepto Doctrinal: Actividades Ciberelectromagnéticas"

(CEMA), en el Ejército de Tierra de los Estados Unidos". Disponible en *http://estudiosmilitares.es/comunicaciones/Pedro%20Cortés%20Ruiz.pdf*

- Corn, Gary, Colonel, "Tallinn Manual 2.0 – Advancing the Conversation", Disponible en: *https://www.justsecurity.org/37812/tallinn-manual-2-0-advancing-conversation/*
- Cornish Paul, Livingstone, David, Clemente, Dave and Yorke, Claire, "On CyberWarfare, A Chatham House Report", Disponible en *https://www.chathamhouse.org/sites/files/chathamhouse/public/Research/International%20Security/r1110_cyberwarfare.pdf.*
- Cross, Tom, Deception for the Cyber Defender; Disponible en: *https://shmoo.gitbooks.io/2015-shmoocon-proceedings/content/bring/02_deception_for_the_cyber_defender.html*
- Crowell, Richard M., "War in the Information Age: A Primer for Cyberspace Operations in 21st Century Warfare", Disponible en: *http://oai.dtic.mil/oai/oai?&verb=getRecord&metadataPrefix=html&identifier=ADA514490*
- Crowell, Richard M.; Some Principles of Cyber Warfare; The United States Naval War College; Joint Military Operations Department;
- Coughlan, Shane M., "Is there a common understanding of what constitutes cyber warfare?" Disponible en Internet en: *http://www.opendawn.com/ewar/docs/is_there_a_common_understanding_of_what_constitutes_cyber_warfare_.pdf*
- Coz Fernández, José Ramón, "Francia, un liderazgo en ciberdefensa" Disponible en *https://ismsforumspain.wordpress.com/2014/10/21/francia-un-liderazgo-en-ciberdefensa/*
- Darczewska, Jolanta, "The Anatomy of Russian Information Warfare: The Crimean Operation, a case Study", Centre for Eastern Studies, May 2014, Disponible en *http://www.osw.waw.pl/sites/default/files/the_anatomy_of_russian_information_warfare.pdf*
- Darczewska, Jolanta, "The devil is in the details: Information Warfare in the light of Russia's Military Doctrine, Point of View, Number 50, Warsaw, May 2015, Disponible en: *https://www.osw.waw.pl/sites/default/files/pw_50_ang_the-devil-is-in_net.pdf*
- de Vergara Evergisto, Las operaciones de Información, artículo publicado en la página web del IEEBA Disponible en *http://www.IEEBA.com*
- Deeks, Ashley, "Tallinn 2.0 and a Chinese View on the Tallinn Process". Disponible en *http://www.lawfareblog.com/tallinn-20-and-chinese-view-tallinn-process*
- de Vergara Evergisto, "Las operaciones de Información". Disponible en *http://www.IEEBA.com*
- Dunlap Charlie, "Cyber Operations and the New Defense Department Law of War Manual: Initial Impressions", Disponible en *http://www.lawfareblog.com/cyber-operations-and-new-defense-department-law-war-manual-initial-impressions.*
- Eidman, Christopher R., "Unconventional cyber warfare: cyber opportunities in unconventional warfare", Monterrey, California: Naval Postgraduate School. Disponible en *http://calhoun.nps.edu/bitstream/handle/10945/42615/14Jun_Eidman_Green.pdf?sequence=1.*
- Eissa, Sergio G., Gastaldi, Sol, Poczynok, Iván y Zacarías Di Tullio, María Elina, "El ciberespacio y sus implicancias en la defensa nacional. Aproximaciones al caso

argentino", Disponible en *http://sedici.unlp.edu.ar/bitstream/handle/10915/40210/Documento_completo.pdf?sequence=1*

- Even, Shmuel y Siman Tov, David, "Cyberwarfare, Concepts and Strategic Trends", Disponible en *https://www.files.ethz.ch/isn/152953/INSS%20Memorandum_MAY2012_Nr117.pdf*
- Farmer, David B. Major, USAF, "Do the Principles of War Apply to Cyber War? Disponible en *https://www. handle.dtic.mil/100.2/ADA522972*
- Feliú Ortega, Luis, "La Confusa Terminología de la Seguridad y la Defensa", Instituto Español de Estudios Estratégicos, "Documento de Opinión" 06/2012. Disponible en *http://www.ieee.es/en/Galerias/fichero/docs_opinion/2012/DIEEEO06-2012_ConfusaTerminologia_Seg.Def._GB_Feliu.pdf*
- Feliú Ortega, Luis, "El espacio cibernético nuevo escenario de confrontación", Cuadernos del CESEDEN. Disponible en Internet *http://www.defensa.gob.es/ceseden/Galerias/destacados/publicaciones/monografias/ficheros/126_EL_ESPACIO CIBERNÉTICO_NUEVO_ESCENARIO_DE_CONFRONTACION.pdf*
- Feliú Ortega, Luis, "Seguridad Nacional y Ciberdefensa, una aproximación conceptual". Disponible en Internet *http://catedraisdefe.etsit.upm.es/wp-content/uploads/2013/01/Ponencia-Luis-Feliu.pdf*
- FitzGerald, Ben and Wright, Parker Lt Col, USAF, "Digital Theaters: Decentralizing Cyber Command and Control". Disponible en *http://www.cnas.org/sites/default/files/publications-pdf/CNAS_DigitalTheaters_FitzGeraldWright.pdf*
- Fojón Chamorro, Enrique, "El Estado Islámico y la guerra cibernética", Blog del Real Instituto Elcano, 20 abril 2015. Disponible en Internet *http://www.blog.rielcano.org/estado-islamicoy-guerra cibernética/*
- Fojón Chamorro, Enrique, Hernández Llorente, Adolfo y Colom Piella, Guillem, "Las redes sociales como herramienta de comunicación estratégica de las Fuerzas de Defensa de Israel durante la operación Pilar Defensivo en Gaza". Disponible en http:*//www.realinstitutoelcano.org/wps/portal/rielcano/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_es/zonas_es/ari94-2012_fojon-hernandez-colom_redes_sociales_israel_pilar_defensivo.*
- Fojón Chamorro Enrique y Colom Piella, Guillem, "Las redes sociales y sus riesgos para las Fuerzas Armadas"; artículo del Diario El Mundo, España, 22 octubre 2014. Disponible en *http://www.elmundo.es/tecnologia/2014/10/22/5447427cca474150258b456c.html*
- Garamone, Jim; "Russian Aircraft Flies Near U.S. Navy Ship in Black Sea" American Forces Press Service *http://www.defense.gov/news/newsarticle.aspx?id=122052*
- Gómez de Ágreda Ángel "Integrando lo "Ciber" en las Operaciones"; Revista de Aeronáutica y Astronáutica; Nº 846; P. 720; 2015; Disponible en *http://publicaciones.defensa.gob.es/pprevistas/be4ba46b-fb63-65ab-9bdd-ff0000451707/index.html#/18/*
- Greylogic, Report. 20 March 2009, *http://www.scribd.com/doc/13442963/Project-Grey-Goose-Phase-II-Report*
- Guillem, Colom, Director de THIBER, the cybersecurity Think Tank, Ciber Elcano, Informe mensual de ciberseguridad, diciembre 2016, Nº 20 P 11. Disponile en: *http://*

www.realinstitutoelcano.org/wps/portal/rielcano_es/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_es/zonas_es/ciber-elcano-20-diciembre-2016

- Herr, Trey and Herrick, Drew, Military Cyber Operations: A Primer, The American Foreign Policy Council, Defense Technology Program Brief, January 2016, Washington DC, # 14, Disponible en: *https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2725275*
- Hoffman, Bruce, "The Use of the Internet by Islamic Extremists" Testimony presented to the House Permanent Select Committee on Intelligence, 4 May 2006, Santa Monica, CA: RAND, 2006. Disponible en *http://www.rand.org/content/dam/rand/pubs/testimonies/2006/RAND_CT262-1.pdf*
- Justribó, Candela, Licenciada. "Ciberdefensa: Una visión desde la UNASUR", Disponible en *http://sedici.unlp.edu.ar/bitstream/handle/10915/44716/Documento_completo.pdf?sequence=1*
- Jayshree, Bajoria, "Libya and the Responsibility to Protect". Disponible en *http://www.cfr.org/libya/libya-responsibility-protect/p24480*
- Karaman, Muhammer, Catalkaya, Hayrettin, Gerehan, Ahmet Zeki and Goztepe, Kerim, "Cyber Operation Planning and Operational Design, Operations and Intelligence". Disponible en *http://r.search.yahoo.com/_ylt=AwrBTvjBa0dXpEcAYnSr9Qt.;_ylu=X3oDMTBydWNmY2MwBGNvbG8DYmYxBHBvcwM0BHZ0aWQDBHNlYwNzcg--/RV=2/RE=1464327234/RO=10/RU=http%3a%2f%2fsdiwc.net%2fdigital-library%2fweb-admin%2fupload-pdf%2f00001773.pdf/RK=0/RS=_VFyxtxDIW_*.LiLIDWfE9VH6kSY-
- Lee, Dave, "Red October' cyber-attack found by Russian researchers". Disponible en *http://www.bbc.com/news/technology-21013087*
- Leed, Maren, "Offensive Cyber Capabilities at the Operational Level: The Way Ahead". Disponible en *https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/130916_Leed_OffensiveCyberCapabilities_Web.pdf*
- Libicki Martin C.; What Is Information Warfare? Strategic Forum; Number 28, May 1995; Disponible en *https://www.questia.com/library/journal/1G1-129891565/what-is-information-warfare.*
- Liles, Samuel, Rogers, Marcus, Dietz, J. Eric and Larson, Dean, "Applying Traditional Military Principles to Cyber Warfare", 2012 4th International Conference on Cyber Conflict, C. Czosseck, R. Ottis, K. Ziolkowski (Eds.), 2012 © NATO CCD COE Publications, Tallinn. Disponible en *https://ccdcoe.org/sites/default/files/multimedia/pdf/3_2_LilesDietzRogersLarson_ApplyingTraditionalMilitaryPrinciplesToCyberWarfare.pdf*
- Lyons,Siobhan; Typewriters are back, and we have Edward Snowden to thank; Disponible en: *https://www.washingtonpost.com/posteverything/wp/2014/11/12/typewriters-are-back-and-we-have-edward-snowden-to-thank/?utm_term=.5dce58e975c5 Opall-Rome, Barbara, Russian Influence on Hezbollah Raises Red Flag in Israel, November 6, 2016, Disponible en: http://www.defensenews.com/articles/russian-influence-on-hezbollah-raises-red-flag-in-israel*
- Malishevski Nikolai; Syria and Information Warfare; Strategic Culture, Disponible

en *http://www.strategic-culture.org/news/2013/09/23/syria-and-information-warfare.html*

- Masera G. y Ortiz J.U. (2015). Gobernanza de riesgos en la sociedad de la información en Conceptos y lenguajes, en ciencia y tecnología. Ed. Guillermo Cuadrado & Juan Redmond & Rodrigo López O. Valparaíso, Chile. Disponible en *https://www.academia.edu/19403028/Conceptos_y_lenguajes_en_ciencia_y_tecnolog%C3%ADa?auto=download*
- Masters, Jonathan, "What Is Internet Governance?" Disponible en *http://www.cfr.org/Internet-policy/Internet-governance/p32843*
- Melo de Carvalho, Paulo Sergio, "Os Projetos Estratégicos das Forças Armadas: contribuição ao desenvolvimento nacional". Disponible en Internet *www2.camara.leg.br/...paulo-sergio-melo-de-carvalho.../view*
- Melo de Carvalho, Paulo Sergio, "Defesa Cibernética e as Infraestruturas Críticas Nacionais". Disponible en *http://www.eceme.ensino.eb.br/meiramattos/index.php/RMM/issue/view/15*
- Metz, Steven, "It's Time to Begin Thinking About the Principles of Cyberwar". Disponible en *http://www.worldpoliticsreview.com/articles/16354/it-s-time-to-begin-thinking-about-the-principles-of-cyberwar*
- Mills, Elinor, "Demilitarizing cybersecurity (Q&A)". Disponible en *http://www.cnet.com/news/demilitarizing-cybersecurity-qa/*
- Nemiche, Mohamed, "Un Modelo Sistémico de Evolución Social Dual". Disponible en *http://www.uv.es/nemiche/thesis.pdf*
- Ottis, Rain, Lorents Peeter, "Cyberspace: Definition and Implications". Disponible en *https://dumitrudumbrava.files.wordpress.com/2012/01/cyberspace-definition-and-implications.pdf*
- Palacios, José Miguel, "La doctrina Gerasimov: segunda entrega", 11 de abril de 2016, Análisis GESI, 7/2016. Disponible en: *http://www.seguridadinternacional.es/?q=es/print/802*
- Parks, Raymond C. and Duggan, David P., "Principles of Cyber-warfare". Disponible en *https://www.researchgate.net/publication/224259524_Principles_of_Cyberwarfare*
- Paul, Christopher, Porche, Isaac R. III, y Axelband, Elliot, "The Other Quiet Professionals Lessons for Future Cyber Forces from the Evolution of Special Forces". Disponible en *http://www.rand.org/pubs/research_reports/RR780.html*
- Perdomo González, Celso, "Inteligencia y Ciberdefensa, nuevos paradigmas en las Estrategias de Seguridad Nacional". Disponible en Internet *http://www.aecpa.es/uploads/files/modules/congress/11/papers/870.pdf*
- Pisanti Baruch, Alejandro, "Gobernanza de Internet y los principios multistakeholder de la Cumbre Mundial de la Sociedad de la Información". Disponible en *http://portal.sre.gob.mx/imr/pdf/Pisanty.pdf*
- Poole, Matthew E. Maj & Schuette Jason C. LtCol.; "Cyber Electronic Warfare: Closing the operational seams"; Marine Corps Gazette; August 2015; Volume 99, Issue 8; Disponible en *https://www.mca-marines.org/gazette/2015/08/cyber-electronic-warfare#sthash.d2gPXDVS.dpuf*

- Rumer, Eugene B., The Kremlin's Advantage Why Cyberwar Will Continue, Foreign Affairs Snapshot August 2, 2016. Disponible en: *https://www.foreignaffairs.com/articles/russian-federation/2016-08-02/kremlins-advantage.*
- Poole, Matthew & Schuette, Jason, "Cyber Electronic Warfare." Marine Corps Gazette. Disponible en *https://www.mca-marines.org/gazette/2015/08/cyber-electronic-warfare*
- Porche, Isaac R. III, Paul, Christopher, York, Michael, Serena, Chad C., Sollinger, Jerry M., Axelband, Elliot, Daehner, Endy M. and Bruce J. Held, "Redefining Information Warfare Boundaries for an Army in a Wireless World". Disponible en *http://www.rand.org/pubs/monographs/MG1113.html*
- Prisco, Nicholas E. MAJ, USA, "The Criticality of Cyber Defense to Operational Commanders". Disponible en *http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA564067*
- Radio Free Europe Liberty, Russia's Shock and Awe: Moscow Ups Its Information Warfare in Syria Operation. Disponible en *http://www.rferl.org/content/russia-syria-shock-awe-military-air-strikes-information-warfare/27293854.html*
- RAND Corporation, "Cyberwarfare". Disponible en *http://www.rand.org/topics/cyber-warfare.html*
- Raymond, David, Cross, Tom, Conti, Gregory and Nowatkowski, Michael, "Key Terrain in Cyberspace: Seeking the High Ground". Disponible en *https://ccdcoe.org/sites/default/files/multimedia/pdf/d2r1s8_raymondcross.pdf*
- Rogers, Robin, "Gestión de Inteligencia en las Américas". Disponible en Internet *http://ni-u.edu/ni_press/pdf/Intel_en_las_Americas.pdf*
- Reilly, Robert R., "Information Operations: Successes and Failures", febrero 2015, Disponible en *http://www.westminster-institute.org/articles/information-operations-successes-and-failures/*
- Rivera, Jason, "A Theory of Cyberwarfare: Political and Military Objectives, Lines of Communication, and Targets", Georgetown's Security Studies Review, Disponible en *http://georgetownsecuritystudiesreview.org/2014/06/10/a-theory-of-cyberwarfare-political-and-military-objectives-lines-of-communication-and-targets/*
- RT News, "Information warfare? Russia accused of killing civilians in Syria", Disponible en *https://www.rt.com/news/317170-russia-accused-civilians-syria/*
- Reilly, Robert R. Information Operations: Successes and Failures; Westminster Institute; febrero 2015, Disponible en *http://www.westminster-institute.org/articles/information-operations-successes-and-failures/*
- Shane, Harris, "How Did Syria's Hacker Army Suddenly Get So Good?" Disponible en *http://foreignpolicy.com/2013/09/04/how-did-syrias-hacker-army-suddenly-get-so-good/*
- Sierra, Daniel, "Las dos caras de la tecnología" Opinión Ciberelcano, Informe mensual de ciberseguridad, abril 2015 / Nº 2. Disponible en *http://www.realinstitutoelcano.org/wps/portal/web/rielcano_es/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_es/zonas_es/ciber-elcano-02-abril-2015/&utm_source=ciberelcano2&utm_medium=email&utm_campaign=abril2015*
- Slideshare Inc, "Cyber Overview on Information Operations", Disponible en *http://www.slideshare.net/lkcyber/cyber-overview-of-information-operations*

- Snoddy, David W., Lt Col, USAF, "A Case for Principles of Cyberspace Operations". Disponible en *https://www.researchgate.net/publication/235142916_A_Case_for_Principles_of_Cyberspace_Operations*
- Sutton, Walter S., Lieutenant Colonel, "Cyber Operations and the Warfighting Functions". Disponible en *www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA590297.*
- Theohary, Catherine A. y Harrington, Anne I., "Cyber Operations in DOD Policy and Plans: Issues for Congress, January 5, 2015". Disponible en Internet *https://www.hsdl.org/?view&did=761572*
- Theohary, Catherine A. y Rollins, John "Terrorist Use of the Internet: Information Operations in Cyberspace" March 8, 2011 Congressional Research Service Disponible en *https://www.fas.org/sgp/crs/terror/R41674.pdf*
- Thomas, Timothy L. Hezballah, Israel, and Cyber PSYOP, Winter 2007, Disponible en: h*ttp://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA465336.*
- Troncoso Javier, "Gobierno de Chile planea crear una Política Nacional de Ciberseguridad". Disponible en *http://www.ohmygeek.net/2015/11/27/chile-politica-nacional-ciberseguridad/.*
- Smith, David J., "Russian Cyber Capabilities, Policy and Practice". Disponible en *http://www.jewishpolicycenter.org/2013/12/31/russian-cyber-capabilities/*
- Unger, Alon, "UAVs - A Tactical Resource or a Strategic Asset?" Disponible en *http://www.israeldefense.co.il/en/content/uavs-tactical-resource-or-strategic-asset*
- Uzal, Roberto, "Lavado Transnacional de Activos en el Espacio cibernético". Disponible en *http://44jaiio.sadio.org.ar/sites/default/files/Programa%2044%20JAIIO.pdf*
- Uzal, Roberto, "Política de Defensa y Política Cibernética de Brasil". Disponible en *http://espacioestrategico.blogspot.com.ar/2013/01/brasil-y-su-politica-cibernetica-de.html*
- Uzal, Roberto, Riesco, Daniel, Montejano, Germán y Berón, Mario; Planeamiento Estratégico Informático: Planeamiento Basado en Capacidades aplicado al Planeamiento Estratégico de la Ciberdefensa, 7mo Simposio Argentino de Informática en el Estado - SIE 2013
- Watson, Ivan, "Cyberwar explodes in Syria". Disponible en *http://edition.cnn.com/2011/11/22/world/meast/syria-cyberwar/index.html*
- Wortzel, Larry M., "The Chinese People's Liberation Army and Information Warfare". Disponible en *http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA596797.*
- Vipond, Alexander Understanding the Cyber Threat: Defence, Response, Democracy, Australian Strategic Policy Institute, 6 Feb 2017, Disponible en: *https://www.aspistrategist.org.au/understanding-cyber-threat-defence-response-democracy/?utm_medium=email&utm_campaign=Daily%20The%20Strategist&utm_content=Daily%20The%20Strategist+CID_5b2c66017d55f36455c4e623d035156f&utm_source=CampaignMonitor&utm_term=Understanding%20the%20cyber%20threat%20defence%20response%20democracyShare*
- Virden, Roy John, "Critical Vulnerability: Defending the Decisive Point of United States Computer Networked Information Systems". Disponible en *http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA415365*

- Watson, Ivan, CNN; Cyberwar explodes in Syria; Disponible en *http://edition.cnn.com/2011/11/22/world/meast/syria-cyberwar/index.html.*
- Wentz, Larry. K., Operaciones de Información de Coalición: la experiencia IFOR, Disponible en: h*ttp://argentina.afceachapters.org/wp-content/uploads/2013/11/OPERACIONES2.pdf*
- Wilson Clay; Information Operations, Electronic Warfare, and Cyberwar: Capabilities and Related Policy Issues; Naval History and Heritage Command; Disponible en *http://www.history.navy.mil/research/library/online-reading-room/title-list-alphabetically/i/information-operations-electronic-warfare-and-cyberwar.html#int*
- Yuill Jim, Feer Fred, Denning Dorothy, "Designing Deception Operations for Computer Network Defense". Disponible en *http://faculty.nps.edu/dedennin/publications/Designing%20Deception%20Operarations%20for%20CND.pdf*
- Zetter, Kim, Researchers Hack Air-Gapped Computer with Simple Cell Phone, 07.27.15. 07.27.15, Disponible en: *https://www.wired.com/2015/07/researchers-hack-air-gapped-computer-simple-cell-phone/*

Periódicos

- Krekel, Bryan, Adams, Patton and George Bakos, "Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage", *The Washington Post,* March 7, 2012. Disponible en *https://www.washingtonpost.com/r/2010-019/WashingtonPost/2012/03/08/National-Security/Graphics/USCC_Report_Chinese_Capabilities_for_Computer_Network_Operations_and_Cyber_%20Espionage.pdf*
- Blasco, Jaime, diario El País, España, "El más fuerte es el más vulnerable", 7 febrero 2015. Disponible en *http://internacional.elpais.com/internacional/2015/02/07/actualidad/1423330690_981628.html*
- Diario El País, Sección Internacional, artículo *Un ciberataque afecta a millones de funcionarios en EEUU,* 5 junio 2015, Disponible en *http://internacional.elpais.com/internacional/2015/06/05/actualidad/1433458231_191963.html*
- Diario La Nación, "Otra amenaza de EI filtran sus hackers datos de 100 marines", 23 marzo 2015. Disponible en *http://www.lanacion.com.ar/1778425-otra-amenaza-de-ei-filtran-sus-hackers-datos-de-100-marines.*
- Diario La Nación Síntesis, "Rice y Powell son investigados por el uso del mail personal", 06 febrero 2016, Página 10, Disponible en Internet: *http://www.lanacion.com.ar/1868716-sin-titulo.*
- Gordon, Michael R. "La estrategia militar innovadora del Kremlin desconcierta a todos"; La Nación, Edición impresa, 23/04/2014 – P. 2
- Elola, Joseba, diario El País, España, 7 febrero 2015, "Así es un ataque, paso a paso" Disponible en *http://internacional.elpais.com/internacional/2015/02/06/actualidad/1423238838_807110.html*
- Febbro, Eduardo, diario Página 12, "Rusia y Occidente aceleran su guerra cibernética". Disponible en *http://www.pagina12.com.ar/diario/elmundo/4-256329-2014-09-28.html*

- Fojón Chamorro, Enrique y Colom Piella, Guillem, "Las redes sociales y sus riesgos para las Fuerzas Armadas", diario El Mundo, España, 22 octubre 2014. Disponible en *http://www.elmundo.es/tecnologia/2014/10/22/5447427cca474150258b456c.html*
- Rueda, Fernando, "Preparados para la guerra cibernética", diario El Tiempo, España, 12 febrero 2013. Disponible en *http://www.tiempodehoy.com/espana/preparados-para-la-guerra cibernética*
- Sanger, David E., "U.S. Cyberattacks Target ISIS in a New Line of Combat", New York Times, April 24, 2016, Disponible en *http://www.nytimes.com/2016/04/25/us/politics/us-directs-cyberweapons-at-isis-for-first-time.html?_r=0*
- Schmitt, Eric & Shanker, Thom. "U.S. Debated Cyberwarfare in Attack Plan on Libya", diario New York Times, oct 17, 2011. Disponible en Internet *http://www.nytimes.com/2011/10/18/world/africa/cyber-warfare-against-libya-was-debated-by-us.html?_r=1*
- Schindler, John, "False Flags: The Kremlin's Hidden Cyber Hand", The Observer Digital Newspaper. Disponible en h*ttp://observer.com/2016/06/false-flags-the-kremlins-hidden-cyber-hand/*
- Tecnología, "Crean una Comisión Nacional para la gobernanza de Internet" diario La Nación", artículo del 23 de abril de 2014. Disponible en *http://www.lanacion.com.ar/1684422-Crean-una-Comisión-nacional-para-la-gobernanza-de-Internet.*
- Tecnología, "¿Quién gobierna Internet?", diario La Nación, artículo del 6 agosto 2015. Disponible en *http://www.lanacion.com.ar/1816509-quien-gobierna -Internet*
- Tecnología, "Una gran familia llamada Internet", diario La Nación, articulo del 27 de enero de 2003. Disponible en *http://www.lanacion.com.ar/468808-una-gran-familia-llamada-Internet*
- The Huffington Post, "Cyber Attacks Caused Brazil Power Outages", 18 marzo 2010. Disponible en *http://www.huffingtonpost.com/2009/11/07/cyber-attacks-caused-braz_n_349530.html*

Manuales y Reglamentos

- República Argentina, *Glosario de Términos de Empleo Militar para la Acción Militar Conjunta,* Proyecto 2015, PC 00-02.
- Ministerio de Defensa, Estado Mayor Conjunto de las Fuerzas Armadas, *Planeamiento para la Acción Militar Conjunta Nivel Operacional,* Proyecto 2015, PC 20-01.
- Ministerio de Defensa, Estado Mayor Conjunto de las Fuerzas Armadas, Planeamiento para la Acción Militar Conjunta Nivel Estratégico Militar", Proyecto, Público, Edición 2008, PC 20 – 09.

Documentos oficiales

Estados Unidos de Norteamérica

- The White House, *The National Security Strategy Report,* May 2010.
- The White House, *International Strategy for Cyberspace 2011.*

- The White House, *National Security Strategy Report 2015.*
- The Judge Advocate General's Legal Center and School, *Operational Law Handbook: 2015.*
- US Department of Defense, *The National Military Strategy 2011.*
- US Department of Defense, *"DOD Report Cyber Attacks Could Elicit Military Response,"* November 16, 2011.
- US Department of Defense, *Política de Defensa para el Hemisferio Occidental,* octubre 2012.
- US Department of Defense, *Law of War Manual,* Office of General Counsel Department of Defense, June 2015
- US Department of Homeland Security, *US Infrastructure Protection Plan.*
- US Director of National Intelligence, *The National Intelligence Strategy of the USA,* DNI Office, August 2014.
- US Department of Defense, *The National Military Strategy 2015.*
- US Department of Defense, *Cyberstrategy 2015.*
- *US Cyber Coast Guard Strategy* June 2015.
- Joint Publication JP-1, *Doctrine for the Armed Forces of the United States,* Washington, 2 May 2007 incorporating change 1, 20 March 2009.
- Joint Publication JP 3-12 (R), *Cyberspace Operations,* Dated 5 February 2013.
- Joint Publication 3-13, *Information Operations,* Dated 27 November 2012 Incorporating Change 1, 20 November 2014.
- Headquarters Department of the Army Washington, DC 26 September 2014AR 530–1 Operations Security.
- Marine Corps, *Concept for Cyberspace Operations,* 9 October 2015, Version 2.0.
- US Army, FM 3-38, *Cyber Electromagnetic Activities,* 2014 US Army.
- The United States Army's *"Cyberspace Operations Concept Capability Plan 2016-2028"* 22 February 2010
- Navy New OPSEC Policy.

Organismos internacionales

- Organización de Estados Americanos, Comité Interamericano contra el Terrorismo, *Declaración de Panamá sobre la Protección de la Infraestructura Crítica en el hemisferio frente al terrorismo 2007.*
- Organización de Estados Americanos, *Informe seguridad cibernética e infraestructuras críticas en las Américas 2015.*
- Organización de Estados Americanos, *Tendencias de Seguridad Cibernética en América Latina y el Caribe,* Publicado en junio de 2014.
- Unión Internacional de Telecomunicaciones, Decisiones destacadas de Guadalajara; *Ciberseguridad*

Reino de España

- Gobierno de España, Presidencia del Gobierno, *Estrategia de Ciberseguridad Nacional,* 2013.

- Gobierno de España, Ministerio de Defensa, *Orden Ministerial 10/2013 de 19 de febrero. por la que se crea el Mando Conjunto de Ciberdefensa de las Fuerzas Armadas.*
- Gobierno de España, Ministerio de la Presidencia, *Ley 36/2015, de 28 de septiembre, de Seguridad Nacional.*
- Ministerio De Defensa, Cuadernos De Estrategia, Instituto Español de Estudios Estratégicos, Instituto Universitario "General Gutiérrez Mellado", *Ciberseguridad. Retos y Amenazas a la Seguridad Nacional en el Espacio cibernético* diciembre 2010
- Ministerio de Defensa de España, Centro Superior de Estudios de la Defensa Nacional (CESEDEN), Documentos de Seguridad y Defensa 44, *Adaptación de la Fuerza Conjunta a la Guerra Asimétrica,* septiembre de 2011,

Reino Unido de Gran Bretaña

- UK Cabinet Office, *The UK Cyber Security Strategy Protecting and promoting the UK in a digital world*
- HM Government, *A Strong Britain in an Age of Uncertainty: The National Security Strategy.*
- HM Government, *National Security Strategy and Strategic Defence and Security Review 2015 A Secure and Prosperous United Kingdom.*

República Argentina

- Ministerio de Defensa, Decreto 2645/2014, *Directiva de Política de Defensa Nacional.*
- Decreto 1729/2007, *Ciclo de Planeamiento de la Defensa Nacional.*

República de Chile

- *Libro de la Defensa Nacional de Chile 2010.*

República de Colombia

- Consejo Nacional de Política Económica y Social, Departamento Nacional de Planeación, *Lineamientos de Política para Ciberseguridad y Ciberdefensa",* 14 de julio de 2011.

República de Ecuador

- Comando Conjunto de las Fuerzas Armadas Dirección de Educación y Doctrina Militar *Manual de Operaciones de Información.* Resolución 14 de agosto de 2014 Disponible en: http://es.slideshare.net/kaluco/manual-de-operaciones-de-informacin-resolucin-14-diedmild003-del-14-de-agosto-de-2014

República de Francia

- Direction de l'information légale et administrative, *Livre Blanc Défense et Sécurité Nationale – 2013.*
- Secrétariat général de la défense et de la sécurité nationale ; *Le plan Vigipirate.*
- Centre interarmées de concepts, de doctrines et d'expérimentations, *Les systèmes d'information et de communication (SIC) en opérations,* Doctrine interarmées DIA-6_ SIC-OPS (2014) N° 147/DEF/CICDE/NP du 24 juin 2014 Amendée le 16 janvier 2016.

República del Perú

- *Libro Blanco de la Defensa Nacional del Perú.*

República Federativa de Brasil

- Ministerio da Defesa, *Política Nacional de Defensa, Estratégia Nacional de Defesa*
- Portaria Normativa No- 3.389/MD, *Política Cibernética de Defensa.*
- Portaria Normativa nº 1.688/MD, de 5 de agosto de 2015, *Política de Segurança da Informação e Comunicações da Administração Central do Ministério da Defesa*
  Ministerio de Defensa de Brasil, Doutrina de Operações Conjuntas – MD30-M-01 / Volumes 1, Año 2011.
- *Estrategia General de Tecnología de la Información y las Comunicaciones (EGTIC) 2015*
- Gabinete de Seguridad, *Estrategia de Seguridad de la Información y las Comunicaciones y de Seguridad Cibernética de la Administración Pública Federal 2015-2018.*
- Ministério Da Defesa do Brasil, *Doutrina Militar de Defesa,* 2007, MD51-M-04.
- Ministerio da Defesa, *Doutrina Militar do Defesa Cibernética,* (1ª Edição /2014), MD 31 M 07.
- *Livro Branco de Defesa Nacional.*
- Ministério da Defesa, *Glossário das Forças Armadas,* MD 35-G-01, 4a Edição 2007.
- Ministério da Defesa, *Doutrina de Operações Conjuntas 1o Volume,* MD41-M-01, 1ª Edição 2011,
- Ministério Da Defesa, *Doutrina de Operações Conjuntas, 2o Volume,* MD30-M-01, 1ª Edição 2011.

GLOSARIO DE TÉRMINOS DEL ÁMBITO TECNOLÓGICO ASOCIADOS A LOS ATAQUES CIBERNÉTICOS

Tradicionalmente el *Malware* ha sido diseñado para infectar ordenadores y redes de computadoras. Sin embargo, la popularidad creciente de teléfonos inteligentes, tablets y otras tecnologías con acceso a Internet proporcionan nuevos y atractivos destinos para los desarrolladores de *malware*. Algunos *malware* combinan atributos en lo que ha dado en llamarse "amenazas combinadas" que son difíciles de detectar y eliminar.

Hacker. "Se le decía así a una persona que investigaba, que llevaba los sistemas más allá de lo pueden dar. Bill Gates es considerado un hacker, el que desarrolló Linux, también". Luego, "El nombre hackers se fue tirando para el lado oscuro, como alguien que entra en una red, roba información y después la vende"[584].

Malware, o software malicioso: genéricamente son herramientas de software diseñadas para interferir o dañar el funcionamiento de otras computadoras y redes; los más populares son los denominados troyanos, bombas lógicas, virus y gusanos, que pueden ser instalados en otras computadoras mediante *chipping, hacking*[585] o simplemente, a través de correos electrónicos.

1. Tipos de *malware*:

a. **Virus**: es un programa que se replica a sí mismo; normalmente se adosa a un programa legítimo de la computadora que es atacado, modificando el programa contagiado y los otros programas de la computadora, así como propagándose hacia otras computadoras.

584 Diario La Nación, Cabot, Diego, Op. Cit.

585 Del inglés hack, hachar. Término utilizado para llamar a una persona con grandes conocimientos en informática y telecomunicaciones y que los utiliza con un determinado objetivo. Este objetivo puede o no ser maligno o ilegal. Hoy tiene una connotación negativa, porque se lo relaciona a tareas ilegales.

b. **Gusanos**: se replica en su totalidad en otras computadoras, pero a diferencia de un virus, no modifica otros programas, sino que captura las direcciones de contactos de la computadora atacada y envía automáticamente mensajes a través del sistema que, si son abiertos, causan demoras en la operación y eventuales colapsos.

c. ***Botnets***: (también conocido como un ejército de Zombis): es un número de computadoras conectadas a Internet, cuyos propietarios no son conscientes de que se han establecido para futuras transmisiones (que incluyen spam o virus) a otros computadores conectados a Internet. Dicho equipo se conoce como un zombie - en efecto, un equipo "robot" o "bot" que sirve a los deseos de algún originador de spam o virus. La mayoría de los computadores comprometidos de esta manera son los hogareños. Según un informe de la empresa rusa Kaspersky Labs, botnets, no spam, virus o gusanos, actualmente son la amenaza más grande a Internet. Un informe de Symantec llegó a una conclusión similar.

d. **Zombi**: es un botnet basado en una PC hogareña cuyo propietario no es consciente de que el equipo está siendo explotado externamente. La creciente prevalencia de conexiones de alta velocidad hace a los computadores atractivos objetivos de un ataque. Las medidas de seguridad inadecuadas hacen el acceso relativamente fácil para un atacante. Por ejemplo, si un puerto de Internet ha quedado abierto, un Troyano puede alojarse allí para ser activado en el futuro.

e. **Troyanos**: es un fragmento de código aparentemente inocuo que en realidad encubre a un programa dañino (virus y/o gusanos) que permite el acceso remoto a la computadora atacada por parte de un usuario externo.

f. **Bombas lógicas**: son una clase de troyanos destinados a ser ejecutados en determinados tiempos o bajo ciertas circunstancias. Algunos programas pueden haber sido saboteados por los mismos creadores sin darse cuenta. Por ejemplo, en 1984 y con la tecnología informática disponible en aquel entonces, la Compañía *Adobe Systems Inc,* accidentalmente incluyó una "bomba lógica" en una versión de su programa popular de *Photoshop*. Esta "bomba lógica" del programa causaba que éste dejara de funcionar después de una fecha en particular y había sido incluido dentro del código para forzar a los que tenían la versión de prueba a comprar la versión final. Sencillamente, los vendedores del programa final se olvidaron de quitarlo.[586] Esas "bombas lógicas" son las que están incluidas en la mayoría de los programas de versión libre, que dejan de funcionar luego de un tiempo. Cuando se compra la versión, lo que hace el vendedor es desactivar esa bomba lógica.

---

586 Greenberg, Lawrence T. y otros, "Information Warfare and International Law", National Defense University, Institute for National Strategic Studies, ISBN 1-57906-001-3, Washington DC EEUU, Año 1998, P. 61 y 62.

g. ***Spyware***: es un software que recopila información de un ordenador sin el permiso o conocimiento del usuario y lo envía al fabricante. Esto puede ser para fines maliciosos o comerciales.

h. ***Rootkits***: es una técnica o conjunto de herramientas utilizadas para ocultar la presencia de *malware* u obtener acceso privilegiado a un ordenador, a veces mediante una "puerta trasera". El sistema operativo del equipo no puede mostrar ningún signo del *rootkit* y puede permanecer indetectado por largos períodos, incluso indefinidamente. Los atacantes pueden utilizar ese acceso privilegiado para realizar otras actividades maliciosas, extraer datos o atacar otras máquinas.

i. ***Exploits***: Se trata de programas maliciosos que contienen datos o códigos ejecutables que se aprovechan de las vulnerabilidades del software ejecutado en un equipo local o remoto. Al utilizar un navegador, hay vulnerabilidades que permiten ejecutar "un código arbitrario" (por ejemplo: instalar y abrir un programa malicioso) en el sistema sin el consentimiento del usuario. A menudo, el primer paso de los atacantes es el de habilitar la escalada de privilegios, para poder realizar cualquier acción en el sistema atacado.

j. ***Ransomware***: es un ataque informático que restringe al usuario el acceso a determinados archivos o sitios, y exige un rescate (*ransom*) a cambio de liberar la clave. El rescate se paga normalmente a través de la moneda virtual bitcoins.

2. Formas y técnicas de un ciberataque:

Ingeniería social: es la manipulación de personas para llevar a cabo acciones específicas o divulgar la información. La información obtenida se utiliza con frecuencia como un habilitador de ataques cibernéticos. En la medida que los adversarios comprenden cómo un individuo hace uso de Internet hay una amenaza mayor para esa persona a través de sus interacciones en línea. La seguridad de las operaciones (OPSEC) es particularmente susceptible a las herramientas y técnicas de ingeniería social dado que explotan, a nivel personal, el conocimiento de la manera en que usan Facebook, mientras que, en las operaciones, dando detalles de dónde están y lo han estado haciendo.

a. Técnicas de Ingeniería Social:

- ***Phishing***: es una forma de intentar adquirir información como nombres de usuario, contraseñas y datos de tarjetas de crédito haciéndose pasar como una entidad confiable en un correo electrónico. Típicamente implica la falsificación de correos electrónicos o dirigir a los usuarios a ingresar datos en un sitio web falso cuya apariencia es casi idéntica a la legítima. *Phishing* es una palabra del in-

glés que se origina de su homófona "*fishing*", que significa 'pesca', en alusión al objetivo del *phishing*: pescar datos, ver "quién muerde el anzuelo".

- ***Spear fishing***: es un intento fraudulento de tratar de suplantar un correo electrónico en contra de una organización específica, buscando acceder de forma no autorizada a datos confidenciales. Estos intentos son más propensos a llevarse a cabo por perpetradores que buscan beneficios financieros, secretos comerciales o información militar y no por "hackers al azar". Esta es la técnica más común que utilizan los chinos para llevar a cabo ataques cibernéticos dirigidos. El objetivo recibe un correo electrónico con un adjunto malicioso o un enlace a una descarga de *malware*. El *malware* crea una puerta de acceso en el sistema, permitiéndole al adversario libre acceso en el futuro evitando todas las defensas. Dos características son fundamentales: el ataque aumenta la probabilidad de que el blanco haga clic en un enlace malicioso y los ataques de "día cero" permiten la creación de puertas traseras incluso en presencia de sofisticadas defensas. El *Spear phishing* normalmente no es ejecutado por hackers al azar, sino llevado a cabo para obtener un beneficio financiero o de espionaje.

- ***Whaling***: (caza de ballenas) es un tipo específico de *hacking* malicioso dentro de la categoría más general que es el *phishing*. Se trata de la caza de datos que pueden utilizarse por el hacker para apuntar específicamente los ataques de *phishing* contra ejecutivos y otros objetivos de alto perfil dentro de las empresas.

- ***Fake email***: un falso (*fake*) correo electrónico es enviado a la víctima, a la cual se persuade para que abra un archivo adjunto o un enlace. Esto a su vez expande malware o dirige a la víctima a un sitio web falso. Lo más probable que ocurra es que la víctima abrirá los archivos adjuntos o links del correo electrónico.

- ***Baiting***: (hostigamiento) el atacante simplemente pone medios extraíbles, como CD-ROM o dispositivos USB a disposición de la víctima (típicos regalos empresariales de empresas vinculadas con la cibernética o copia de exposiciones). Los medios de comunicación son rotulados de tal manera que provocan interés en los empleados de una organización, los cuales los introducen en sus computadoras por mera curiosidad. Una vez que se ejecuta en un equipo, la carga útil de dichos dispositivos, que generalmente funcionará automáticamente, permite el acceso remoto de malware a la computadora.

- ***Telephone***: la víctima es llamada por teléfono por un individuo que se hace pasar por alguien con autoridad como para persuadir a la víctima para que realice una determinada tarea. Los procedimientos más comunes son aquellos en los que los delincuentes se disfrazan como un empleado del proveedor de Internet de la víctima o de Microsoft y lo "advierte" de un problema ficticio en su computadora. La víctima suele ser inducida a: realizar alteraciones en su sistema informático

para debilitar sus defensas; navegar a un sitio web que permite el acceso remoto; navegar a un sitio web para descargar *malware* (con el pretexto de un supuesto problema o descargar protección de virus); o entregar información personal o de sus tarjetas de crédito.

- ***Social networking***: (redes sociales) las redes sociales ofrecen una serie de oportunidades para la ingeniería social. Algunos usuarios de redes sociales o de correos electrónicos han sido blanco de mensajes que fingen ser de un amigo que está en el extranjero y que necesita dinero para poder regresar a su país. Cuando se responde, la víctima es desviada a una página web donde se le solicita información personal. Los criminales explotan otros medios sociales para descubrir los intereses de la víctima. Este conocimiento se utiliza para atacar sus mensajes de destino o tweets con enlaces integrados a *malware*. Apuntar también a correos o tweets que ofrecen una manera de conseguir más adeptos y a menudo desvían a las víctimas a sitios web que descargan malware.

3. Los efectos de un malware pueden incluir:

a. **Ataques de denegación de servicio (DoS)**: el objetivo es inundar a la red que se toma como blanco con requerimientos para sobrecargarlo y así incapacitarlo. Cuando este ataque DoS se lleva a cabo por un número importante de computadoras, se denomina Denegación de Servicio Distribuida (DDoS, por su sigla en inglés). Eso pasó en Estonia en el año 2007, y en el peor ataque cibernético que registra la historia el 27 de marzo de 2013. Aquí, la disputa entre dos empresas: *Spamhouse*, que tiene sede en Londres y en Ginebra, y se dedica a crear listas negras de los que envían publicidad no solicitada (o spam), añadió a sus bloqueos a *Cyberbunker*, una firma holandesa que ofrece alojamiento para toda clase de contenidos "excepto" – aseguran – pornografía infantil y terrorismo. La respuesta fue un ataque que puso a *Spamhouse* fuera de combate. Pero eso fue solo el principio. Por la técnica de ataque utilizada, los efectos se propagaron por la infraestructura de Internet, haciendo que el acceso a la Web, entre otras cosas, funcionara muy lentamente. En particular, además de *Spamhouse*, se vio afectado un servicio esencial para la Web, llamado DNS.

   Por diversos motivos, los servidores DNS pueden ser objeto de ataques informáticos. El problema es que si la traducción de la dirección URL (*Uniform Resource Locator, o dirección web*) que se teclea en la computadora y que es convertida a números IP por el DNS falla o se demora, Internet o deja de funcionar o se pone demasiado lenta. En corto lapso, un ataque Distribuido de Denegación de Servicio (DDoS) envía simultáneamente millones de solicitudes de página al sitio que, por lo tanto, se inunda de tráfico y deja de responder. Para esto se usan computadoras personales infectadas con un tipo de software malicioso llamado *botnet*

(sigla en inglés por red de robots). Los *botnets* les entregan el control remoto de las PC infectadas a los atacantes. Son una pesadilla para los administradores de sistemas y uno de los negocios más ricos de los delincuentes informáticos, que alquilan el tiempo de estas redes para los DDoS, el envío de virus y la distribución del *spam*. Una nueva técnica, denominada *reflexión del DNS* aumenta la sobrecarga de las redes y sistemas.[587]

b. **Geo localización de *Smartphones, Tablets, Laptops* u otros dispositivos similares.**
Normalmente, los equipos que sólo están conectados directamente a un *router* pueden acceder a la dirección MAC. Sin embargo, el hacker lo hace aparecer como si la petición proviene de una PC conectada al *router* y no a un sitio Web.

La función de geo-ubicación dentro del navegador Firefox de Mozilla, que tiene acceso a la base de datos de los servicios de localización de Google que contienen información recogida por los vehículos de Google Street View, puede utilizarse para vincular las direcciones MAC con coordenadas GPS y, de esa manera, identificar la ubicación del *router* utilizado para acceder a la Web.

c. **Explotación de redes sociales.**
No es que los atacantes abusen de la información publicada en las redes sociales o que estén librando ataques en dichos sitios; el problema es que normalmente no se entienden los riesgos asociados con la información que se publica en Facebook, Twitter, y no se advierte la magnitud de los daños que pueden producirse debido a un ataque que fuese exitoso.

4. Técnicas para introducir malware

a. ***Chipping***: acción de introducir *chips* subrepticiamente en una computadora, para explotar sus debilidades o defectos. Un *chip* es un circuito integrado por muchos transistores, en cuyo interior pueden llegar a existir incluso millones de estos, arreglados entre sí para ejecutar muchas funciones; su composición sobre todo es de silicio. Existen *chips* diseñados para miles de tareas electrónicas.

b. ***Spoofing***: en términos de seguridad de redes hace referencia al uso de técnicas de suplantación de identidad o *Phishing* a través de las cuales un atacante, generalmente con fines maliciosos o de exploración se hace pasar por una entidad distinta a través de la falsificación de los datos en una comunicación.

---

587 Puede encontrarse una explicación más técnica en el artículo (en idioma inglés) de Afilias, Global Registry Services, Abley Joe, Nairobi, mayo de 2006; Disponible en: http://ws.edu.isoc.org/data/2006/570066312448cfa2c134a4/060515.AfNOG-DNS-DDOS.pdf

Se pueden clasificar los ataques de *spoofing*, en función de la tecnología utilizada. Entre ellos se encuentra el IP *spoofing* (quizás el más conocido), ARP *spoofing*, DNS *spoofing*, Web *spoofing* o *email spoofing*, aunque en general se puede englobar dentro de *spoofing* cualquier tecnología de red susceptible de sufrir suplantaciones de identidad.

c. **Protocolo de resolución de direcciones** (ARP, del inglés *Address Resolution Protocol*) es un protocolo de comunicaciones de la capa de red, responsable de encontrar la dirección de hardware (Ethernet MAC) que corresponde a una determinada dirección IP.

d. ***Zero Day*** (también conocido como hora cero o *0-day*): es una vulnerabilidad divulgada de software de computadora que los hackers pueden explotar para afectar adversamente programas de computadoras, datos, equipos adicionales o una red. Se conoce como un "día cero" porque una vez que se conoce la falla, el autor del software tiene cero días para planificar y asesorar cualquier mitigación contra su explotación (por ejemplo, por asesoramiento, soluciones o mediante la emisión de parches).

e. **Mal direccionamiento**: (*Misdirection* en inglés - *Maskirovka* en ruso) en lugar de designar a una máquina o servidor para que sea atacado, se plantan datos falsos en cada extremo y en el punto de entrada en red – diseñados para ser prácticamente indistinguibles de los reales e invisibles para los usuarios regulares. Mientras que los hackers pueden traspasar otras medidas de defensa, inmediatamente son mal dirigidos hacia ese sistema simulado.

d. ***Honey spots***: es una herramienta de la seguridad informática dispuesto en una red o sistema informático para ser el objetivo de un posible ataque informático, y así poder detectarlo y obtener información de este y del atacante.

e. **Inhibidores conocedores de protocolo** (*protocol aware jammers*): interfieren la red con el conocimiento del protocolo; una manera de interrumpir una red inalámbrica es generar un ruido continuo de alta potencia en todo el ancho de banda cerca de los nodos de transmisión o recepción. El dispositivo que genera tal ruido se llama *jammer* y el proceso *jamming*. De conocerse el protocolo, el *jamming* puede hacerse más eficiente en lo que respecta a la necesidad de energía y menos detectable si es capaz de interrumpir brevemente los paquetes de control seleccionados o reducir a cero el rendimiento de la red, si fuese necesario.

5. Otros términos:

Flame, también conocido como Flamer, sKyWIper y Skywiper, es un malware que ataca ordenadores con el sistema operativo Microsoft Windows. El programa se ha

usado para llevar a cabo ataques de ciber espionaje en países de Oriente Medio. Puede propagarse a otros sistemas a través de la red de área local (LAN) y mediante memorias USB. Puede grabar audio, capturar pantallas, pulsaciones de teclado y tráfico de red. El programa también graba conversaciones de Skype y puede controlar el Bluetooth para intentar obtener información de los dispositivos Bluetooth cercanos. Estos datos, junto con los documentos almacenados en el ordenador, son enviados a uno o varios servidores dispersos alrededor del mundo. Cuando termina, el programa se mantiene a la espera hasta que recibe nuevas instrucciones de esos servidores.

Stuxnet es un gusano informático que afecta a equipos con Windows. Es el primer gusano conocido que espía y reprograma sistemas industriales, en concreto sistemas SCADA de control y monitoreo de procesos, pudiendo afectar a infraestructuras críticas como centrales nucleares. Stuxnet es capaz de reprogramar controladores lógicos programables y ocultar los cambios realizados.

WannaCry ("quiero llorar") es un programa de tipo *ransomware*. Se viraliza a partir de un archivo aparentemente inofensivo que el usuario abre bajo engaño y que al ser ejecutado encripta el contenido de la computadora y exige el pago de un "rescate" para liberarlo a cambio de no hacer públicos los datos. El e-mail urge a la víctima, mediante algún pretexto alarmante, a abrir el adjunto o hacer clic en el link. Casi de inmediato aparece un cuadro que anuncia que los archivos del equipo han sido cifrados, así como las instrucciones para pagar el rescate y recibir la contraseña para descifrarlos. El virus afecta a computadores que usan el sistema operativo de Microsoft y sus programas más populares como Word o Excel.

ANEXOS

Objetivos estratégicos y líneas de acción de una Política de Ciberdefensa

FIGURA 18: CÉLULA TEÓRICA DE OPERACIONES DE INFORMACIÓN[588]

MODELO 1	MODELO 2
Desarrollar las capacidades operacionales conjuntas de ciberdefensa en la dimensión ciberespacial.	Formar FFAA conscientes de los riesgos derivados de las amenazas cibernéticas de tal forma de obtener fuerzas listas y capacitadas para accionar en este dominio.
Incrementar la seguridad de la información y comunicaciones en el ámbito conjunto;	Potenciar las capacidades de prevención, detección, reacción, análisis, recuperación, respuesta, investigación y coordinación frente a las actividades que perturben en el espacio cibernético la normal ejecución de las operaciones militares.
Promover la capacitación del personal en materia de ciberdefensa;	Construir y mantener alianzas y asociaciones internacionales para disuadir amenazas comunes y aumentar la seguridad en el ambiente cibernético internacional.
Reforzar el sistema de Investigación y Desarrollo (I&D) de las Fuerzas Armadas en materia de ciberdefensa;	Asegurar los Sistemas de Información y Comunicaciones que constituyen las Infraestructuras Críticas de las FFAA y todas aquellas infraestructuras estratégicas que determine el Poder Ejecutivo Nacional
Desarrollar y mantener actualizada la doctrina de ciberdefensa.	Alcanzar y mantener los conocimientos, habilidades, experiencia y capacidades tecnológicas que se necesitan para sustentar todos los objetivos de defensa cibernética.
Potenciar la cooperación con diferentes órganos con capacidad de respuesta ante incidentes cibernéticos en aspectos de interés común.	

588 Fuente: Elaboración propia.

Modelo 1

La definición de los objetivos estratégicos y la determinación de las líneas de acción obedecen a los siguientes fundamentos básicos:

a. Las actividades de ciberdefensa estarán orientadas para atender las necesidades de la Defensa Nacional;
b. Las acciones de ciberdefensa en el ámbito de las Fuerzas Armadas tienen como objetivo asegurar el uso del espacio cibernético, impidiendo o dificultando su uso contra los intereses propios y garantizando, de esa forma, la libertad de acción.
c. La Seguridad de las Tecnologías de la Información y Comunicaciones (TICs) es la base de la ciberdefensa y depende directamente del reconocimiento de la importancia de construir y mantener la confianza en los sistemas TIC´s que conforman el Instrumento Militar, lo que conlleva a asegurar que sus miembros conozcan los riesgos de operar en el espacio cibernético y posean los conocimientos y el acceso a las herramientas que posibilitan su protección.
d. La capacitación tecnológica y la Investigación y Desarrollo en materia de ciberdefensa, deberá ser buscada de manera armónica con la Política que establezca la Secretaría de Ciencia, Tecnología y Producción para la Defensa del Ministerio de Defensa a través de la Subsecretaría de Ciberdefensa.

Objetivos Estratégicos

En función de lo expuesto, los objetivos que se deberán lograr para cumplir con la finalidad impuesta son los siguientes:

1. Desarrollar las capacidades operacionales conjuntas de ciberdefensa en la dimensión ciberespacial;
2. Incrementar la seguridad de la información y comunicaciones en el ámbito conjunto;
3. Promover la capacitación del personal en materia de ciberdefensa;
4. Reforzar el sistema de Investigación y Desarrollo (I&D) de las Fuerzas Armadas en materia de ciberdefensa;
5. Desarrollar y mantener actualizada la doctrina de ciberdefensa; y
6. Potenciar la cooperación con diferentes órganos con capacidad de respuesta ante incidentes cibernéticos en aspectos de interés común.
7. Para el logro de estos objetivos, resulta imprescindible potenciar un marco de aplicación coherente, integrado por una doctrina de ciberdefensa, procedimientos y normas técnicas que ayuden a garantizar la protección de la información, sus sistemas y servicios, así como de las redes que los soportan.

Líneas de acción relacionadas con los objetivos estratégicos

Las líneas de acción explicitan las actividades a ser implementadas para alcanzar los objetivos estratégicos.

Líneas de acción pertenecientes al Objetivo Estratégico 1: Desarrollar las capacidades operacionales conjuntas de ciberdefensa en la dimensión ciberespacial;

Desarrollar las capacidades conjuntas de prevención, defensa, detección, análisis, respuesta, recuperación y coordinación frente a las actividades que perturben en el espacio cibernético la normal ejecución de las operaciones de las Fuerzas Armadas, haciendo énfasis en las Tecnologías de la Información y Comunicaciones (TICs), las capacidades militares de defensa y otros sistemas de interés nacional.

a. Desarrollar un plan de capacidades operacionales en la dimensión ciberespacial, descomponiendo cada una de ellas en los elementos que las conforman, – Material – Infraestructura – Recursos humanos – Información – Logística – Adiestramiento – Doctrina – Organización;
b. Desarrollar y mantener actualizadas las instrucciones de prevención y respuesta ante agresiones cibernéticas;
c. Ampliar y mejorar las capacidades del Equipo de Respuesta ante Emergencias Informáticas (CERT);
d. Asegurar la cooperación de los organismos con responsabilidades en ciberseguridad, en especial entre el CERT de la Administración Pública y el Comando Conjunto de Ciberdefensa de las Fuerzas Armadas;
e. Desarrollar modelos de análisis y evaluación de las técnicas empleadas por las ciberamenazas desarrollando medidas de protección de los activos, servicios y sistemas de las Fuerzas Armadas.

Líneas de acción pertenecientes al Objetivo Estratégico 2: Incrementar la seguridad de la información y comunicaciones en el ámbito conjunto;

Garantizar la implementación de un esquema de seguridad de la información y comunicaciones en el ámbito conjunto a fin de reforzar las capacidades de detección, la seguridad y la resiliencia de las infraestructuras y redes y mejorar la protección de los sistemas clasificados.

a. Implementar una arquitectura de seguridad y establecer las normas, que permitan crear un entorno seguro para el normal funcionamiento de las redes utilizadas por las Tecnologías de la Información y Comunicaciones (TICs), las capacidades militares de defensa y otros sistemas de interés nacional;
b. Evaluar y garantizar la eficacia de las redes utilizadas por las Fuerzas Armadas en el desarrollo de las operaciones, mitigando todas las vulnerabilidades conocidas;
c. Impulsar el desarrollo de estándares en seguridad de la información y comunicaciones a través de los organismos y entidades de normalización y certificación nacionales y promover su adopción;
d. Desarrollar modelos de simulación que permitan analizar las dependencias entre las diferentes Infraestructuras Críticas y los riesgos acumulados por éstas;

e. Optimizar el modelo de interconexión de los organismos dependientes de las Fuerzas Armadas a las redes públicas de voz y datos, maximizando su eficacia, disponibilidad y seguridad; y
f. Establecer las normas de contratación y adquisición del equipamiento y software a ser utilizado en el ambiente de la ciberdefensa.

Líneas de acción pertenecientes al Objetivo Estratégico 3: Promover la capacitación del personal en materia de ciberdefensa;

Alcanzar y mantener los conocimientos, habilidades, experiencia y capacidades tecnológicas que se necesitan para sustentar los objetivos de ciberdefensa.

a. Definir los perfiles de personal necesarios para conducir las actividades de ciberdefensa; desarrollar un Plan de Carrera.
b. Crear cargos y funciones específicas con personal especializado para conducir las actividades de ciberdefensa, estableciendo criterios y controlando sus traslados;
c. Identificar, registrar y seleccionar al personal con competencias y habilidades, existentes en los ámbitos interno o externo de las Fuerzas Armadas, para integrar el sector de ciberdefensa;
d. Capacitar personal, de forma continua, para actuar en ciberdefensa, bajo la orientación del Comando Conjunto de Ciberdefensa, aprovechando las estructuras existentes;
e. Fomentar la participación de personal de ciberdefensa en cursos, etapas, congresos, seminarios, simposios y otras actividades similares relacionadas en el país o en el exterior;
f. Crear instrumentos para hacer viable y motivar la permanencia de personal especializado en ciberdefensa, permitiendo la continuidad de sus actividades; e
g. Incluir el contenido de defensa cibernética en las currículas de los cursos, de todos los niveles, de los establecimientos de educación del Ministerio de Defensa.

Líneas de acción pertenecientes al Objetivo Estratégico 4:
Reforzar el sistema de Investigación y Desarrollo (I&D) de las Fuerzas Armadas en materia de ciberseguridad:

Adecuar las estructuras de Investigación y Desarrollo de las tres Fuerzas Armadas para atender las necesidades de la ciberdefensa.

a. Planificar y ejecutar la adecuación de las estructuras de Investigación y Desarrollo, integrando los esfuerzos entre las Fuerzas Armadas para satisfacer las necesidades de la ciberdefensa;
b. Determinar las necesidades de ciberdefensa, del área de Investigación y Desarrollo, en el ámbito de la Defensa, para identificar las capacidades científico-tecnológicas necesarias para el desarrollo del sector;

c. Impulsar modelos y técnicas de análisis de ciberamenazas y medidas de protección de productos, servicios y sistemas, así como su especificación, evaluación y certificación;
d. Crear un Laboratorio de Investigación y Desarrollo con responsabilidad en la homologación del hardware, firmware y sistemas que se deberán utilizar en la implementación de la subcapacidad de ciberdefensa.

Líneas de acción pertenecientes al Objetivo Estratégico 5: Desarrollar y mantener actualizada la doctrina de ciberdefensa:

a. Crear la doctrina de ciberdefensa conjunta a propuesta del Comando Conjunto de Ciberdefensa;
b. Fomentar el desarrollo y/ o intercambio de tesis, disertaciones y otros trabajos similares, con enfoque doctrinario, en instituciones de enseñanza superior civiles y militares de interés para las actividades de ciberdefensa;
c. Promover el intercambio doctrinario, normativo y técnico, con instituciones civiles y militares, nacionales y de naciones amigas;
d. Insertar la defensa cibernética en ejercicios de simulación y en las ejercitaciones conjuntas;
e. Crear un sistema de gestión de conocimiento de lecciones aprendidas para la composición y actualización de la doctrina; y
f. Designar al Comando Conjunto de Ciberdefensa como responsable de proponer las innovaciones y actualizaciones a la doctrina de ciberdefensa en el ámbito de las Fuerzas Armadas.

Líneas de acción pertenecientes al Objetivo Estratégico 6: Potenciar la cooperación con diferentes órganos con capacidad de respuesta ante incidentes cibernéticos en aspectos de común interés;

Promover las mejores prácticas en el conocimiento de la situación, la alerta y la respuesta ante incidentes cibernéticos.

a. Promover la cooperación entre los organismos de ciberdefensa y los elementos de ciberseguridad de la Administración Pública Nacional y sectores privados;
b. Impulsar ejercicios de simulación de incidentes en el ambiente cibernético en el que participen todos los elementos de ciberseguridad de la Nación, promoviendo si fuese necesario, la participación del sector privado en estos;
c. Promover la cooperación con los sectores público y privado, promoviendo el intercambio de información sobre vulnerabilidades, ciberamenazas y sus posibles consecuencias, especialmente en lo relativo a la protección de los sistemas de defensa.

Modelo 2:

Supuestos

La definición de los objetivos y la determinación de líneas de acción de la Política de Defensa Cibernética Nacional para cada uno de ellos, obedecen a los siguientes supuestos básicos:

a. Las actividades de defensa cibernética en el Ministerio de Defensa están orientadas para atender las necesidades de la Defensa Nacional;
b. Es necesario considerar el carácter transfronterizo de las amenazas por lo que será esencial promover la cooperación regional y global, ya que muchas de las posibles medidas que se adopten sólo resultarán eficaces si se adoptan internacionalmente con la adecuada cooperación y coordinación entre los distintos países.
c. Las medidas que se adopten en materia de defensa cibernética, deberán estar alineadas con los requisitos que regulan la Protección de las Infraestructuras Críticas;
d. La eficacia de las acciones de Defensa Cibernética del Ministerio de Defensa depende directamente del grado de concientización alcanzado junto con las organizaciones e individuos sobre el valor de la información que procesan;
e. El espacio cibernético puede usarse como una herramienta para llevar a cabo Operaciones de Información y operaciones cibernéticas en computadoras, y redes de computadoras. La seguridad de la Información y Comunicaciones que depende de los individuos es la base de la defensa cibernética.
f. La gestión eficaz de los riesgos derivados del espacio cibernético debe edificarse sobre una sólida cultura de seguridad en las redes. Ello requiere de los usuarios una sensibilización respecto de los riesgos que entraña operar en este medio, así como el conocimiento de las herramientas para la protección de su información, sistemas y servicios.

Objetivos estratégicos

En función de lo expuesto y las pautas emanadas del Poder Ejecutivo Nacional / Ministerio de Defensa, los objetivos que se deberán llevar a cabo para cumplir con la finalidad impuesta son los siguientes:

1. Formar Fuerzas Armadas conscientes de los riesgos derivados de las amenazas cibernéticas de tal forma de obtener fuerzas listas y capacitadas para accionar en este dominio.
2. Asegurar los Sistemas de Información y Comunicaciones que constituyen las Infraestructuras Críticas de las Fuerzas Armadas y todas aquellas infraestructuras estratégicas que determine el Poder Ejecutivo Nacional.
3. Potenciar las capacidades de prevención, detección, reacción, análisis, recuperación, respuesta, investigación y coordinación frente a las actividades que perturben en el espacio cibernético la normal ejecución de las operaciones militares.

4. Construir y mantener alianzas y asociaciones internacionales para disuadir amenazas comunes y aumentar la seguridad en el ambiente cibernético internacional.
5. Alcanzar y mantener los conocimientos, habilidades, experiencia y capacidades tecnológicas que se necesitan para sustentar todos los objetivos de defensa cibernética.

Líneas de acción relacionadas con los objetivos estratégicos

Al Objetivo Estratégico Nº 1: *Formar Fuerzas Armadas conscientes de los riesgos derivados de las amenazas cibernéticas de tal forma de obtener fuerzas listas y capacitadas para accionar en este dominio.*

Este objetivo tiene como propósito reclutar, formar y capacitar continuamente a personal especialista en defensa cibernética, tanto en e strategia y conducción como en aspectos técnicos. A su vez, también requiere concientizar a los miembros que integran las Fuerzas Armadas y que no participan directamente en operaciones de defensa cibernética, sobre la importancia de la seguridad en el espacio cibernético y del uso responsable de las nuevas tecnologías.

Para alcanzar este objetivo se deberán adecuar, potenciar y/o desarrollar las medidas que a continuación se detallan:

a. Implementar el reclutamiento, formación y retención del personal militar y civil asignado al ámbito de la defensa cibernética.
b. Mantener un Plan de Carrera que incluya formación y perfeccionamiento permanente a lo largo de ella.
c. Desarrollar programas de concientización en Seguridad Cibernética.
d. Fomentar el desarrollo de buenas prácticas de mecanismos y técnicas para el uso seguro de las TIC.
e. Desarrollar e implementar programas de intercambio con el sector privado con experto en seguridad cibernética y TIC.

Al Objetivo Estratégico Nº 2: *Asegurar los Sistemas de Información y Comunicaciones que constituyen las Infraestructuras Críticas de las Fuerzas Armadas y todas aquellas infraestructuras estratégicas que determine el Poder Ejecutivo Nacional.*

Se deberá identificar, priorizar y defender todas aquellas redes, sistemas, procesos y datos que permitan llevar a cabo misiones eficientes, incrementando su resiliencia.

Para alcanzar este objetivo se deberán adecuar, potenciar y/o desarrollar las medidas que a continuación se detallan:

a. Implementar una arquitectura de seguridad y redactar las normativas pertinen-

tes, que permitan crear un entorno seguro para el normal funcionamiento de las redes utilizadas por las IC y las Fuerzas Armadas.
b. Monitorear, analizar, evaluar y garantizar la eficacia de las redes utilizadas por las Fuerzas Armadas en el desarrollo de las operaciones mitigando todas las vulnerabilidades conocidas.
c. Desarrollar e implementar los Planes de Defensa de las Redes utilizadas en el ámbito de Defensa Nacional, así como también los Planes de Resiliencia / Continuidad de las operaciones
d. Analizar las exigencias de interoperabilidad inter fuerzas de los equipamientos cibernéticos de los niveles operacional y superiores.
e. Elaborar Ejercicios de Simulación de Incidentes en el espacio cibernético en el que participen todos los elementos de seguridad cibernética nacionales promoviendo si fuese necesario, la participación del sector privado.
f. Optimizar el modelo de interconexión de los organismos dependientes de las Fuerzas Armadas a las redes públicas de voz y datos, maximizando su eficacia, disponibilidad y seguridad.
g. Establecer las normas de contratación y adquisición del equipamiento y software a ser utilizado en el ambiente de la defensa cibernética.
h. Elaborar doctrina conjunta y eventualmente combinada en materia de seguridad y defensa en el ámbito de la defensa cibernética

Al Objetivo Estratégico Nº 3: *Potenciar las capacidades de prevención, detección, reacción, análisis, recuperación, respuesta, investigación y coordinación frente a las actividades que perturben en el espacio cibernético la normal ejecución de las operaciones militares.*

Para alcanzar este objetivo se deberán adecuar, potenciar y/o desarrollar las medidas que a continuación se detallan:

a. Ampliar y mejorar las capacidades de detección, análisis y atribución de las amenazas cibernéticas.
b. Desarrollar y mantener actualizadas las contingencias de incidentes cibernéticas y sus instrucciones de prevención y respuesta.
c. Desarrollar modelos de análisis y evaluación de las técnicas empleadas por las amenazas cibernéticas desarrollando medidas de protección de los activos, servicios y sistemas de las Fuerzas Armadas.
d. Elaborar un Programa de Ejercicios de Simulación de Incidentes de seguridad cibernética.
e. Mejorar la capacidad de prevención, detección, respuesta y recuperación de incidentes con los proveedores de servicios y la administración pública.

Al Objetivo Estratégico Nº 4: *Construir y mantener alianzas y asociaciones internacionales para disuadir amenazas comunes y aumentar la seguridad en el ambiente cibernético internacional.*

Para alcanzar este objetivo se deberán adecuar, potenciar y/o desarrollar las medidas que a continuación se detallan:

a. Incrementar la presencia en organizaciones y foros internacionales y regionales sobre seguridad en el espacio cibernético.
b. Propiciar la suscripción de acuerdos con organizaciones internacionales y con los principales socios regionales.
c. Participar en el establecimiento de canales internacionales de información, detección y respuesta.
d. Participar y promover en forma coordinada la realización de ejercicios de defensa cibernética con los principales socios regionales y globales.

Al Objetivo Estratégico Nº 5: *Alcanzar y mantener los conocimientos, habilidades, experiencia y capacidades tecnológicas que se necesitan para sustentar todos los objetivos de defensa cibernética.*

Para alcanzar este objetivo se deberán adecuar, potenciar y/o desarrollar las medidas que a continuación se detallan:

a. Adaptar los procedimientos a cumplir en el ámbito de la defensa cibernética al plexo legal vigente tanto a nivel nacional como internacional.
b. Potenciar las capacidades con el fin de lograr ejercer una respuesta oportuna, legítima y proporcionada en el espacio cibernético ante amenazas o agresiones que puedan afectar a la Defensa Nacional.
c. Promover la adopción de estándares en ciberseguridad desarrollados por organismos y entidades de normalización y certificación nacionales e internacionales.

Contenido tentativo del Anexo de Operaciones de Información a un Plan de Campaña

Si bien muchos elementos del espacio cibernético podrán ser ubicados geográficamente en los dominios físicos, también será necesario tener una completa comprensión de la postura y las capacidades del adversario en este ambiente y conocer qué fuerzas y capacidades propias pueden ser atacadas y cómo. Para ello, durante el análisis de la misión, deberán identificarse las brechas significativas entre lo que se conoce del adversario y otros aspectos relevantes del ambiente operacional para poder formular los Requerimientos de Inteligencia. Deberá recordarse que, aunque un lado ve lo que ve (o piensa que ve) sólo puede adivinar en lo que no puede ver.

Los adversarios en el espacio cibernético pueden ser Estados nacionales, grupos o individuos, y que las partes del espacio cibernético que ellos controlan no necesariamente deberán encontrarse dentro de las fronteras geográficas asociadas con nacionalidad del actor, o proporcionales a la influencia geopolítica del actor. Un grupo delictivo, o un grupo con motivaciones políticas o incluso una persona puede tener una mayor presencia y capacidad en el espacio cibernético que muchas naciones.

Con independencia de qué fase operacional pueda estar en curso, siempre será importante determinar qué autorizaciones se requiere para ejecutar operaciones cibernéticas.

El anexo de Operaciones de Información debe reflejar cuáles son las maneras por las cuales las fuerzas conjuntas pueden integrar las principales capacidades de guerra electrónica, operaciones psicológicas, operaciones de red de computadoras, engaño militar, y seguridad de las operaciones, para influir, alterar, corromper o usurpar el proceso de toma de decisiones humano y/o automatizado del adversario y al mismo tiempo proteger el propio.

Un formato tentativo a un Plan de Campaña dependerá de si el espacio cibernético es considerado un dominio separado, o al carecer de especialistas, sea considerado únicamente trasversal a cada Fuerza Armada.

1. Situación

1.1. **Fuerzas enemigas**: Se identificará la situación del enemigo, la disposición de sus fuerzas, sus elementos de operaciones de información, sus vulnerabilidades, sus capacidades para degradar las fuerzas propias y las posibles acciones que pueda llegar a tomar. Debe describirse el espacio cibernético como aquel que involucra

el uso de capacidades ciberespaciales con el propósito de obtener objetivos en él. También son las que usan computadoras y redes de computadoras y software[589].

1.2. **Fuerzas propias**: Se describirá en líneas generales la arquitectura de las redes de cada Fuerza Armada y su interconexión nodal. No se deben mencionar vulnerabilidades propias. Mencionar la dependencia de redes civiles fuera del control militar que inexorablemente deberán ser usadas.
Identificar posibles situaciones de conflictividad dentro del espectro electromagnético especialmente cuando deban llevarse a cabo operaciones conjuntas o multinacionales. Identificar métodos para reducir los conflictos y priorizar la distribución del espectro.
Identificar personas o grupos clave en el Teatro de Operaciones.
Identificar los medios de operaciones de información agregados y desagregados como así también los recursos disponibles asignados por la estrategia militar.

2. Misión
Según se determine.

3. Ejecución.
a. **Esquema de apoyo**

1. **Concepto de apoyo.** Describir el concepto de apoyo y objetivos de las operaciones de información. Un concepto complejo puede requerir un esquema para mostrar los objetivos de las operaciones de información y las tareas relacionadas. Incluir una descripción sobre el concepto global de las operaciones de información, con los detalles específicos en los apartados o apéndices correspondientes. Este anexo debe contener la información necesaria para sincronizar la oportunidad de cada uno de los elementos/actividades relacionadas con las operaciones de información. Deben incluir además las imposiciones - Qué debe hacer - y las restricciones - Qué no debe hacer - el Comandante.

2. **Operaciones de Seguridad.** Indicar cómo las tareas de OPSEC negarán al enemigo el conocimiento de aquellos aspectos críticos, que, si fuesen conocidos por él, podrían comprometer, hacer fallar o limitar el éxito de la operación y, por lo tanto, deben ser protegidos. Sincronizar este elemento con otros elementos de las operaciones de información. En el apéndice 1, operaciones de seguridad, se podrá brindar información más detallada respecto de estas operaciones.

---

589 A modo de ejemplo se hace notar que, en un conflicto armado, algunas torres específicas de telefonía celular pueden convertirse en piezas clave, dada la necesidad de mantenerlas en pie y funcionando para enviar mensajes de texto clave a la población, mientras que otras pueden ser anuladas o destruidas.

En lo que respecta a la penetración y control del espectro, se hará referencia a las instrucciones de seguridad cibernética de rutina, haciendo hincapié en algunas particulares según el escenario, a saber: dividir el acceso a la información por niveles, no conectar computadoras con información sensible a la red, prohibir el uso de USB, revisar diariamente la página web de amenazas 0-day http://www.zone-h.org/notify/single?zh=1, segmentar la arquitectura de los sistemas, uniformar el uso del explorador XXX y asegurar los parches de seguridad diariamente, usar herramientas sandbox, usar herramientas de detección SSL. Debe ponerse atención en los servidores que tienen acceso a Internet.

3. **Operaciones de apoyo de información militar (ex Operaciones psicológicas).** Indicar cómo se degradará el poder de combate relativo del enemigo, se reducirá la interferencia de civiles, se minimizará el daño colateral y se maximizará el apoyo de la población local a las operaciones en curso. Identificar y priorizar las audiencias y efectos deseados de PSYOP. Sincronizar este elemento con otros elementos de las operaciones de información. Sincronizar este elemento con otros elementos de las operaciones de información. En el apéndice 2, Operaciones de apoyo de información militar, se podrá brindar información más detallada respecto de estas operaciones.

4. **Operaciones de engaño.** Indicar cómo las operaciones de engaño podrán influir o engañar al enemigo. Sincronizar este elemento con otros elementos de las operaciones de información. En el apéndice 3, Operaciones de Engaño, se podrá brindar información más detallada respecto de estas operaciones.

5. **Guerra Electrónica.** Indicar cómo las tareas de guerra electrónica degradarán, interrumpirán, negarán y engañarán al enemigo. Indicar las medidas defensivas y ofensivas de guerra electrónica. Identificar y priorizar los efectos y los blancos. Sincronizar este elemento con otros elementos de las operaciones de información. En el apéndice 4, Guerra Electrónica, se podrá brindar información más detallada respecto de estas operaciones.

6. **Operaciones de red de computadoras.** En el caso de una fuerza conjunta, este párrafo deberá expresarse en términos de operaciones de red de computadoras activas, pasivas y de exploración.

7. **Operaciones de red de computadoras activas.** Determinar cómo las tareas de las operaciones de red de computadoras activas destruirán, degradarán, interrumpirán y negarán al enemigo. Identificar y priorizar los efectos y los blancos. Sincronizar este elemento con otros elementos de las operaciones de información. Elevar los requerimientos a la estrategia militar para su aprobación y aplicación.

8. **Operaciones de red de computadoras pasivas.** Determinar cómo las tareas de las operaciones de red de computadoras pasivas protegerán y defenderán las propias redes de computadoras. Sincronizar este elemento con otros elementos de las operaciones de información. En el Anexo, Comunicaciones y Guerra Electrónica se podrá brindar información más detallada respecto de estas operaciones.

9. **Operaciones de red de computadoras de exploración.** En el caso de una fuerza conjunta, este párrafo establece las tareas y sincronizaciones con otros elementos de las operaciones de información. Elevar los requerimientos a la estrategia militar para su aprobación y aplicación.

Ejemplos Reglas de Empeñamiento para operaciones cibernéticas

- La protección de [designar] infraestructuras críticas contra ataques cibernéticos está autorizada.
- Las medidas de defensa cibernética pasiva como recorrido de redes, *sniffing*, y forensia informática están autorizadas.
- Las medidas de defensa cibernética activas, como introducción de malware, descifrado de códigos, falsificación de páginas web y DoS solo podrán llevarse a cabo con autorización de la estrategia militar.
- Las medidas de defensa cibernética activas sobre terceros países que han sido utilizados para la ejecución de un ataque cibernético, con o sin su autorización, por otro país, no están autorizadas.
- Cuando esté autorizado por (ESPECIFIQUE), están permitidos los ataques a redes de compiutadoras para (ESPECIFIQUE efecto, por ejemplo, destruir, degradar, negar, alterar) en contra de (ESPECIFIQUE sistema(s), por ejemplo, información en computadoras o en redes o las mismas computadoras o redes) de (ESPECIFIQUE estado, actor o sistema, por ejemplo, sistemas gubernamentales, sistemas comerciales, sistemas militares)[590].
- Cuando esté autorizado por (ESPECIFIQUE), la defensa de redes de cómputo en respuesta a actividades no autorizadas dentro de sistemas de información amigos o redes de computo está autorizada[591].
- Cuando esté autorizado por (ESPECIFIQUE), está permitido el aprovechamiento de redes de cómputo en contra de (ESPECIFIQUE blanco) sistemas de información automatizados o redes de cómputo[592].
- Los ataques cibernéticos y "potes de miel" son de responsabilidad de la estrategia Militar previo conocimiento de la Estrategia Nacional.
- El uso de computadores o del ciberespacio para distribuir información está autorizado.
- El introducir datos erróneos o falsos en sistemas propios para ejecutar engaño cibernético está autorizado.

590 Instituto Internacional de Derecho Humanitario, Manual de Reglas de Enfrentamiento, San Remo, noviembre 2009, P. 60 Regla 131 B

591 Ibidem Regla 131 C

592 Ibidem Regla 131 D

- La Seguridad Cibernética está autorizada. Todo *malware* o intrusiones deben ser referidas tan rápido como sea posible al Centro de Operaciones Cibernéticas Conjuntas del Teatro de Operaciones.
- El uso de la fuerza convencional para repeler actos de agresión cibernéticos no está autorizado.
- Las operaciones psicológicas no están autorizadas.
- Las operaciones psicológicas transmitidas a (ESPECIFIQUE audiencia) por (ESPECIFIQUE medio, por ejemplo, canales de radio, canales de televisión, páginas web) están permitidas.
- Las operaciones psicológicas transmitidas a (ESPECIFIQUE audiencia) por (ESPECIFIQUE medio, por ejemplo, canales de radio, canales de televisión, páginas web) están autorizadas[593].
- El uso de (ESPECIFIQUE método, por ejemplo, computadora, correo electrónico y sistemas telefónicos) para comunicar mensajes aprobados a (ESPECIFIQUE audiencia aprobada) está autorizado[594].
- La distribución de panfletos para comunicar mensajes aprobados está permitida.
- Las operaciones cibernéticas DOS en instalaciones cibernéticas ubicadas dentro de los límites geográficos del país no están autorizadas.
- Las operaciones cibernéticas DOS en instalaciones cibernéticas ubicadas dentro de los límites geográficos del país están autorizadas.
- El uso de *botnets* en operaciones de defensa cibernética no está autorizado.
- Los DDoS sobre servidores ISP ubicados geográficamente dentro del país están autorizados.
- Los DDoS sobre servidores ISP ubicados geográficamente fuera del país no están autorizados.
- Las operaciones de Ciberdefensa de NCO cerradas están autorizadas.
- Las estratagemas cibernéticas para fines de defensa cibernética están autorizadas.
- Está autorizado el uso de *sniffers* y *key loggers* para fines de la seguridad informática.
- El ataque a redes de cómputos militares (CNT) o sistemas de cómputos está autorizado.

593 Ibidem Regla 132 B

594 Ibidem Regla 132 C

SOBRE LOS AUTORES

EVERGISTO DE VERGARA, General de División (R). Magíster en Ciencias con especialización en Defensa Nacional de la Universidad de Defensa de los Estados Unidos y tiene un posgrado en Políticas Públicas – Investigación Aplicada de los Institutos de Política de Estados y Gestión Públicas. Actualmente es profesor la Escuela de Guerra Conjunta de las Fuerzas Armadas en las maestrías de Estrategia General y Estrategia Operacional. Autor de numerosas publicaciones, entre las que se destacan: "El arte operacional"; "Quaia Nominor Leo I y II – acerca del Liderazgo en el Ejército"; "Del planeamiento en el Nivel Técnico al Planeamiento en el Nivel Operacional"; "Los niveles de la guerra o el conflicto; Los conflictos en Latinoamérica" y "Clausewitz y el centro de gravedad". Autor del libro Estrategia, Métodos y Rutinas, publicado en 2013.

GUSTAVO ADOLFO TRAMA, Contraalmirante en situación de retiro. Oficial del Estado Mayor de la Armada Argentina. Magíster en Relaciones Internacionales por la Universidad de Belgrano y Master in Arts (Management) por la Universidad Salve Regina, Newport, Rhode Island, Estados Unidos. Autor de diversas publicaciones, entre ellas, "Reglas de Empeñamiento", tomos 1, 2 y 3, editados por la Escuela Superior de Guerra Conjunta. Actualmente se desempeña como profesor asesor en el área de Ejercicios de la Escuela Superior de Guerra Conjunta de las Fuerzas Armadas.