MATERIA: TALLER DE TRABAJO FINAL INTEGRADOR
TRABAJO FINAL INTEGRADOR

TEMA:
CIBEROPERACIONES

TÍTULO:

LAS CIBEROPERACIONES APLICADAS A UN TEATRO DE OPERACIONES – ESTUDIO DE CASO: GUERRA RUSO GEORGIANA

AUTOR: CCIM Sergio Ezequiel SEPETICH

2016

I. TABLA DE CONTENIDOS

II. RESUMEN

Las ciberoperaciones nacieron como casos aislados, cuyo dominio de ocurrencia era el virtual. En 2008 eso cambió y por primera vez una acción cibernética clara fue desarrollada para dar apoyo a una acción militar física. Esta operación marca el punto inicial de las ciberoperaciones como parte integral del esfuerzo bélico y un buen punto de partida para estudiar si las ciberoperaciones pueden comandarse y controlarse en forma centralizada o descentralizada, permitiéndole al Comandante Operacional, en el último caso, retener el control de las ciberoperaciones en su Teatro de Operaciones.

Distintos países han adoptado enfoques distintos para resolver este problema, entonces, sobre la base de aquella primera operación, se ha registrado una evolución. De los países que utilizan las ciberoperaciones en apoyo del accionar militar, Estados Unidos es el que más oficialmente trabaja. Se conoce su doctrina y se han publicado numerosos trabajos de investigación en referencia de los modelos de trabajo empleado.

En la República Argentina el desarrollo de ciberoperaciones se encuentra limitado a las Ciberoperaciones Defensivas y en forma centralizada. Se propone la creación de un sistema descentralizado de comando y control, que permita a los Comandantes de los Teatros de Operaciones, realizar el planeamiento y supervisar la ejecución de sus organismos de ciberoperaciones, dentro de las reglas del diseño operacional.

III. PALABRAS CLAVE.

Ciberoperaciones – Ciberataques – Osetia del Sur – Abjasia – Rusia – Georgia

CONSIDERACIONES INICIALES

Desde la popularización de internet, en la segunda mitad de la década del 90, todos los servicios han migrado su operación, administración, archivo y consultas a ámbitos digitales. En la actualidad, prácticamente toda la gestión, pública y privada funciona de esta forma. El comercio mundial depende de los enlaces de datos digitales e incluso, un porcentaje importante del dinero mundial existe solo digitalmente. En junio de 2014, el Reino Unido de Gran Bretaña expresaba tener un capital total de £404.796.898.206, mientras que el dinero impreso ascendía solamente a £61.409.605.670.

Esto quiere decir que, del total del capital, solo un 15,17% existe físicamente. Dicho en otras palabras, el 84,83% del dinero del Reino Unido no existe físicamente, sino solo en la forma de información en bases de datos y de sus correspondientes bonos reales (Bank of England, 2014).

Todo este cambio de paradigma, que ha incentivado el comercio global y facilitado la ejecución de múltiples aspectos de la gestión, ha abierto todo un nuevo espacio virtual, donde se desarrollan innumerables actividades humanas.

Este espacio pronto se ha convertido, al igual que todos los espacios físicos del planeta, en sujeto de interés por parte de los estados, las empresas, las personas y otras organizaciones y, como sujeto de interés, se ha tornado en origen de conflictos y, finalmente, en un espacio de maniobra.

Al igual que antes, cuando los ejércitos marchaban por los terrenos en pugna entre naciones, reinos e imperios, hoy ejércitos de otra naturaleza, pero con el mismo fin, marchan y operan en este espacio cibernético, el ciberespacio.

Pero no solo se ha ampliado el espectro espacial de la guerra, sino que los objetivos de la guerra hoy incluyen la economía, la opinión pública y la percepción del resto de los estados. Estos y muchos otros aspectos tienen alguna componente inmersa en el ciberespacio.

La economía del mundo está cambiando permanentemente. En la Figura 1 puede observarse en qué porcentaje participan de la economía de los Estados Unidos la agricultura, la industria, los servicios y particularmente los servicios de información. La evolución es obvia. Los Estados Unidos ha dejado atrás a la agricultura e incluso a la industria como actividad principal de la economía (Bell, 1999).

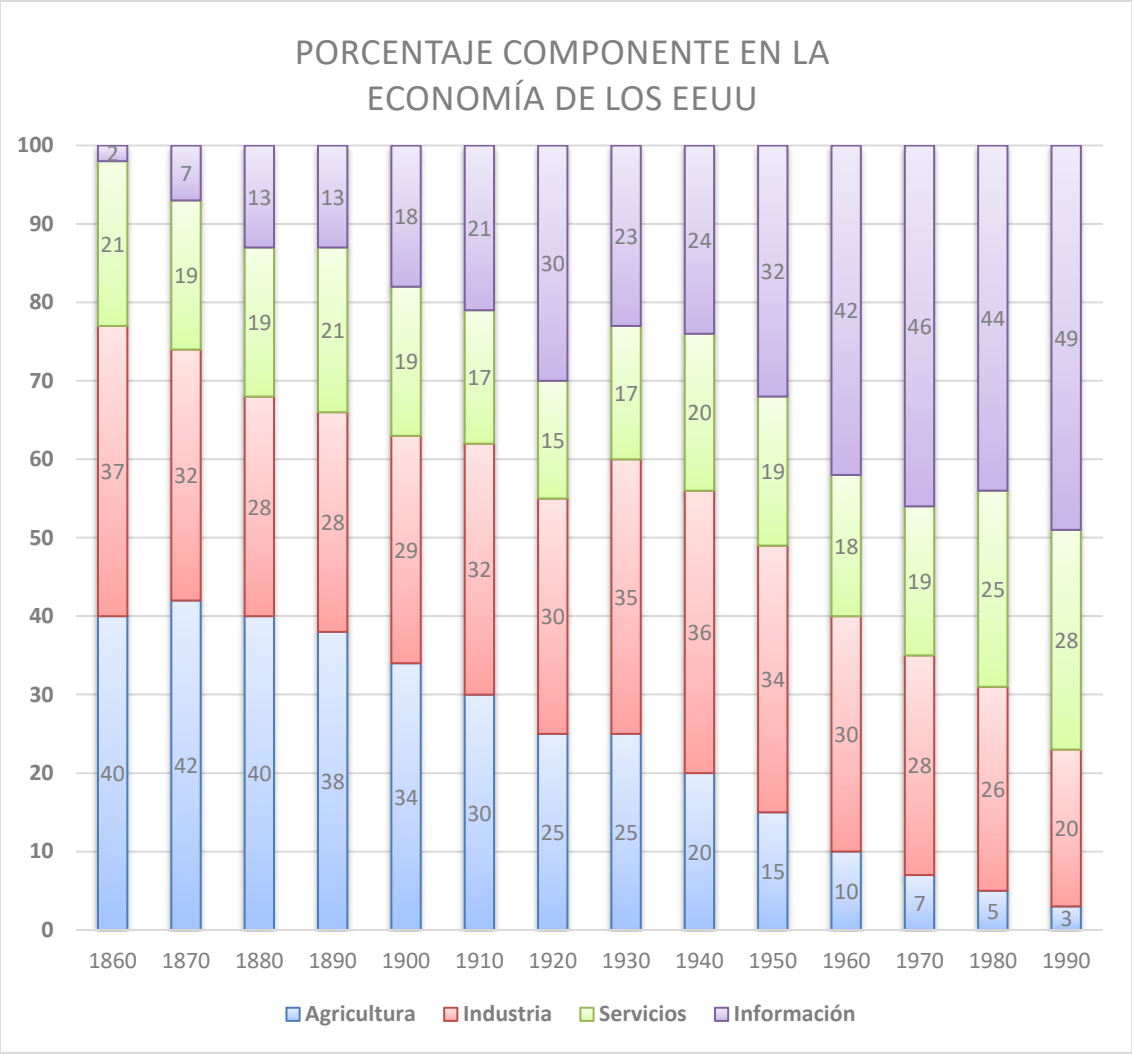

FIGURA 1: Composición porcentual de la economía de los EEUU entre 1860 y 1990 (Bell, 1999).

Este hecho, junto con la popularización de Internet genera que la economía de un país como Estados Unidos depende mayormente de una industria que, a su vez, depende fuertemente de la fortaleza de los sistemas de información. Sistemas de información que ya no están aislados ni son cerrados, sino que todos los sistemas están interconectados, ya sea por Internet o por accesos de red dedicados. Desde una red, puede accederse a otras. Un caso práctico, expuesto por William Ashmore, propone la siguiente situación.

Imagínese que Usted se encuentra en su viaje de trabajo. Se acerca a un cajero automático para retirar los fondos que le permitirán pagar por el alojamiento y comida que ha consumido en su estadía. El cajero se encuentra fuera de servicio. Entonces, usted intenta pagar con tarjeta de crédito, pero los hoteles no pueden procesar su pago, porque el servidor bancario se encuentra saturado de pedidos de información. Entonces usted decide comunicarse con su empleador, pero las redes de teléfonos celulares no funcionan. Los

servidores de correo electrónico se encuentran fuera de servicio y de repente usted se da cuenta que, a pesar de poseer el dinero, no puede conseguir un hotel, ni pagar su comida, ni comprar un pasaje para regresar, ni enviar un mensaje a su jefe informándole la situación. Los efectos de esta situación, a escala nacional son devastadores para la economía (Ashmore, 2009).

Todo lo descripto en el párrafo anterior sucedió en Georgia entre julio y agosto de 2008. Hasta ese momento, las acciones ciberespaciales y las bélicas no habían accionado coordinadamente para el logro de un mismo objetivo. Esto cambió durante el desarrollo de la Guerra Ruso Georgiana o Guerra de Osetia del Sur, que transcurrió en agosto de dicho año. Como se ha dicho, esto no sucedió antes y consideramos conveniente establecer, en esta operación, el cero de las ciberoperaciones en apoyo de una maniobra operacional clásica. Es desde ella que iniciaremos el análisis que nos permitirá establecer la relevancia del control de las ciberoperaciones desde el nivel operacional.

Argentina no ha estado ausente del desarrollo de este tema. Desde el año 2005, en la esfera de la Jefatura de Gabinete de Ministros se crea el "Comité de Seguridad de la Información" (Jefatura de Gabinete de Ministros, 2005) y en 2015, se reglamentan las funciones principales del Comando Conjunto de Ciberdefensa, que se encuentra facultado para desarrollar tareas en el nivel estratégico militar (Ministerio de Defensa, 2015), no habiéndose creado, aún, agencias que permitan implementar o controlar las ciberoperaciones en el nivel operacional.

En nuestro país ya se cuenta con trabajos de investigación escritos en las escuelas de guerra, pero sin una equivalencia en doctrina militar conjunta.

Los trabajos consultados para la realización del presente, son los que se detallan a continuación.

- "Desafíos operacionales en el ciberespacio como nuevo campo de lucha". Mayor Ezequiel Rodríguez Cisneros, 2012.

- "Las vulnerabilidades de las operaciones militares derivadas de las redes sociales en internet". Capitán de Corbeta Augusto Sebastián Rivolta, 2012.

- “Dificultades para la obtención de la sorpresa en el nivel operacional ante el avance de las nuevas tecnologías de la información”. Mayor Juan Martín Barbosa Larronde, 2012.

- “Lineamientos para la seguridad cibernética en un teatro de operaciones”. Capitán de Corbeta Carlos Alberto Giudici, 2013.

- “La guerra cibernética en el nivel operacional”. Capitán de Corbeta Eduardo Pablo Páez, 2014.

i. Planteo del Problema

¿Cómo se planifican y ejecutan las ciberoperaciones militares?

¿Puede ejercerse el comando y control de las ciberoperaciones al nivel operacional?

ii. Alcances y Limitaciones de la Propuesta

En el presente trabajo se realizará un estudio histórico de las ciberoperaciones desarrolladas por Rusia, durante la Guerra de Osetia del Sur, en 2008, pero reconociendo la importancia de las ciberoperaciones desarrolladas en Estonia un año antes por, presumiblemente, las mismas fuerzas rusas y diversos trabajos realizados por autores cuyos países han descentralizado el planeamiento y ejecución de las ciberoperaciones.

El trabajo se limitará a extraer conclusiones referentes a la implementación de las ciberoperaciones en el nivel operacional y se extenderá solamente a otras disciplinas cuyo estudio sea necesario para la implementación de ciberoperaciones en el nivel operacional.

finalmente, este trabajo se refiere a la descentralización del comando y control de las ciberoperaciones en tiempos de guerra, conflicto o crisis. Algunos de los conceptos desarrollados, pueden no aplicarse a tiempos de paz.

iii. Objetivo General

El objetivo general de este trabajo es analizar, a la vista de lo expuesto previamente, las acciones supuestamente desarrolladas por Rusia, para comprender que debe tenerse en cuenta en la doctrina de nivel operacional para el diseño de líneas de operaciones cibernéticas puras o a través del espacio cibernético, en el gran diseño operacional de una campaña, para establecer la viabilidad y utilidad de contar con un organismo, en el nivel operacional, que controle las ciberoperaciones propias y asista en la mitigación de las consecuencias de las ciberoperaciones del oponente.

iv. Objetivos Específicos

- Extraer conclusiones del estudio de las ciberoperaciones efectuados por Rusia, en Georgia en el año 2008, útiles a la implementación de organismos de control en el nivel operacional.
- Estudiar la evolución de las ciberoperaciones desde 2008 hasta el presente, utilizando artículos profesionales de las escuelas de guerra de la Armada, el Ejército y la Fuerza Aérea de los Estados Unidos y artículos periodísticos de revistas especializadas.
- Concluir sobre la conveniencia de la implementación de una agencia de comando y control de ciberoperaciones en el nivel operacional.

v. Metodología

La metodología empleada en esta investigación será de tipo exploratoria y descriptiva. Para este trabajo se realizará un estudio histórico de los ciberataques desarrollados durante la Guerra Ruso Georgiana mediante diversas crónicas y estudios históricos. Para la formulación de conclusiones útiles, se utilizará doctrina escrita por países líderes en el campo y artículos publicados en revistas militares especializadas en los cuales se trata la problemática de las ciberoperaciones.

CAPÍTULO 1: GUERRA RUSO GEORGIANA DE 2008

1. ESTUDIO DE CASO

1.1. Crisis del Soldado de Bronce (2007)

Estonia es una antigua república socialista soviética. En febrero de 1990 se independizó de la URSS, manteniendo un porcentaje de población de origen ruso. Hasta el momento de escribirse el presente trabajo, el porcentaje de población de origen ruso, es del 25.1%. (Estonian Republic Statistics Center, 2016) Este porcentaje de la población estonia se encuentra fuertemente identificada con Rusia, sus valores, tradiciones e historia. (US Central Intelligence Agency, 2016)

FIGURA 2: Mapa de Estonia (www.freeworldmaps.net – 19 de octubre de 2016)

En la capital de Estonia, la Ciudad de Tallinn, se encuentra un monumento, conocido como el Soldado de Bronce de Tallinn. Este monumento ha servido como punto de encuentro cada vez que los ruso-estonios han decidido realizar manifestaciones contra el gobierno de Estonia. Es por esta causa que, en 2007, se decidió que la estatua fuese retirada de su emplazamiento y colocada en un sitio menos público (AFCEA International, 2012). La respuesta de los ruso-estonios se materializó el 27 de abril de 2007, en la forma de protestas que

escalaron en saqueos y destrucción de propiedades públicas y privadas. Todas las demostraciones fueron contenidas y en el transcurso de una semana todos los daños físicos estuvieron reparados (AFCEA International, 2012).

Cuando el conflicto físico hubo terminado, los sitios de la administración de gobierno, los de los bancos y muchos otros sitios de noticias y servicios web fueron sistemáticamente afectados mediante ataques de denegación de servicio.

Estos ataques iniciaron el 27 de abril y se extendieron por espacio de tres semanas. Durante ese lapso distintos servicios como páginas gubernamentales, sistemas bancarios, agencias de noticias y sitios de comercio electrónico estuvieron inoperativos (Richards, 2016).

Estonia se convirtió en el primer estado en reconocer públicamente estar bajo ataque cibernético y comenzó un proceso de migración de sus servicios web, públicos y privados, a servidores en el extranjero. Tan solo seis años después de los ataques, Estonia se ha convertido en un ejemplo de medidas de ciberdefensa y ciberseguridad a nivel nacional (Rehman, 2016).

1.2. Guerra Ruso Georgiana (2008)

1.2.1. Antecedentes de la Guerra

Rusia y Georgia han presentado diferencias desde el inicio del siglo 20. Cuando la Unión Soviética colapsó a principios de los años 90, múltiples líderes, en general representantes regionales y étnicos, reclamaron independencia de los antiguos estados satélites (George, 2009).

Aun cuando las pretensiones de regiones como Abjasia y Osetia del Sur fueron vistas como razonables inicialmente, fueron escalando hasta traspasar los límites que el nuevo gobierno de Tiflis estaba dispuesto a tolerar. Las diferencias escalaban, generando enfrentamientos y posteriormente desescalaban con la misma velocidad. Este ciclo generó un estado de tensión permanente, que era incentivado por Rusia mediante apoyo político al gobierno regional separatista y apoyo logístico a sus ejércitos (AFCEA International, 2012).

En 1992 el parlamente ruso sancionó una ley que permitía a cualquier persona que hubiese sido habitante de cualquiera de las antiguas repúblicas socialistas soviéticas a solicitar la ciudadanía rusa. Esto convirtió a Rusia en un actor importante de cualquier conflicto regional en sus antiguos estados satélites, ya que reclamaba estar actuando por sus ciudadanos (The Christian Science Monitor, 2008).

FIGURA 3: Mapa de Georgia, Osetia del Sur y Abjasia (AFP, 2008)

Desde 1992 hasta 2007 los conflictos entre estas regiones y el gobierno central de Georgia consistieron en incrementos de la presencia de fuerzas armadas y de seguridad de ambos bandos, escalando luego a enfrentamientos de baja intensidad e intercambios de disparos entre patrullas de magnitud pequeña. La presencia de tropas de paz del ejército ruso sirvió como factor estabilizador del nivel de conflicto (AFCEA International, 2012).

En 2008, el presidente de Georgia, Mikheil Saakashvili, estaba procurando el ingreso de Georgia a la OTAN y comenzó una campaña de lucha contra mercados de contrabando, implementando medidas anticorrupción que parecían hechas a medida de Abjasia y Osetia del Sur. Simultáneamente, inició un incremento de las capacidades de su ejército.

	RUSIA	GEORGIA
Tropas	107.000	21.150
Tanques	800	128
Vehículos Blindados de Transporte de Tropas	+2000	135
Aeronaves (ala fija, todos los tipos)	+400	17
Artillería (Autopropulsada y de tiro)	900	109
Helicópteros (todos los tipos)	147	35
Buques de guerra	122	8
Misiles Balísticos de Corto Alcance	+36	0

Tabla 1: Distribución de Fuerzas en el Teatro de Operaciones Georgia

El 1 de agosto un auto de la policía georgiana fue detonado, hiriendo a cinco agentes de policía. Esto generó una serie de enfrentamientos menores que fueron escalando en intensidad en los días subsiguientes, llegando al ataque de artillería de aldeas de pobladores georgianos. El 3 de agosto, las fuerzas rusas comenzaron a tomar posiciones muy cerca de la frontera con Georgia. El Ministro del Interior intentó entablar charlas directas, pero le fue negado el acceso a la capital de Osetia del Sur, Tskhinvalli. Se reunió con el comandante de las tropas georgianas General Qurashvili y el comandante de las fuerzas rusas de mantenimiento de la paz, Coronel Kulakmethov. En declaraciones posteriores, manifestó que el gobierno de Georgia pretendía una solución pacífica, pero sin discutir la soberanía de Georgia sobre Osetia del Sur. Los enfrentamientos seguían escalando entre milicianos osetios y el ejército georgiano. A pesar de que el presidente Saakashvili ordenó un alto el fuego unilateral a sus fuerzas, los ataques a las aldeas georgianas recrudecieron. Ante esto, el 8 de agosto las tropas de Georgia ocuparon la capital de Osetia del Sur y las principales ciudades en respuesta a estos ataques de artillería, provenientes de territorios controlados por los osetios (George, 2009).

Rusia, que se encontraba realizando ejercicios militares en la frontera con Georgia en un alto estado de alerta y alistamiento y con un número de tropas mayor al de las georgianas, respondió la agresión, el mismo 8 de agosto, con una invasión que no tenía precedentes desde la invasión a Afganistán de 1979 (Ziegler, 2011).

El 9 de agosto, se abre un segundo frente, cuando milicianos de Abjasia abren fuego contra tropas georgianas y son apoyadas inmediatamente por fuerzas rusas. A partir de este momento, las fuerzas del ejército de Georgia inician un repliegue que se extenderá hasta el 15 de agosto, cuando los rusos hayan ingresado más de 55 km en el territorio de Georgia (Rojo, 2013).

Finalmente, entre el 22 y el 26 de agosto, las tropas rusas se retiran de Georgia a territorios en Abjasia y Osetia del Sur. El conflicto armado finaliza con el reconocimiento formal y oficial de Rusia a las repúblicas independientes de Osetia del Sur y Abjasia (George, 2009).

1.2.2. Ciberataques

Este conflicto entre Rusia y Georgia, fue distinto de los enfrentamientos anteriores. El gran cambio estuvo materializado por los ataques cibernéticos que la estructura de información, tanto privada como gubernamental, sufrió desde unos días previos al inicio de las acciones. Estos ataques fueron incrementando su intensidad en frecuencia e intensidad a medida que progresaba el conflicto. Si bien Rusia nunca reconoció haber planificado, ejecutado y apoyado la acción contra la estructura de información georgiana, un análisis de cuáles fueron las consecuencias que estos ciberataques generaron deja lugar a muy pocas dudas, con respecto a la responsabilidad rusa en la ejecución o en el apoyo a los ejecutantes (AFCEA International, 2012).

Los análisis posteriores al conflicto demostraron que los ataques fueron preparados con anterioridad a las acciones bélicas, iniciándose el 19 de julio de 2008. Es decir que las acciones contra los sistemas de información dieron inicio, al menos, veinte días antes que Georgia invadiera Osetia del Sur y Abjasia. Por supuesto, el planeamiento de las acciones ejecutadas sobre los sistemas de información de Georgia debe haber empezado mucho antes que esta fecha. (AFCEA International, 2012)

Los ataques principales tomaron la forma de Negación de Servicio Distribuido, Desfiguración Web y Redirección de Tráfico.

- Denegación de Servicio

  Estos ataques consisten en saturar de pedidos al servidor que aloja la página o servicio web. De esta forma el servidor ve saturado su ancho de banda disponible y queda fuera de servicio o, al menos, inaccesible para sus usuarios legítimos. Cuando este ataque se realiza desde una serie de computadoras o redes informáticas de las cuales se ha tomado el control previamente, se denomina Denegación de Servicio Distribuido (US Joint Chief of Staff, 2013).

- Desfiguración (o deformación) web

  Consiste en la colocación en el sitio web atacado contenido que apoye la opinión del atacante (en general contraria a la del propietario del sitio web). En Georgia, el sitio web oficial de presidencia mostraba un montaje de fotos de los principales dictadores del Siglo XX y del presidente de Georgia (Vice Chairman of the Joint Chiefs of Staff, 2012)

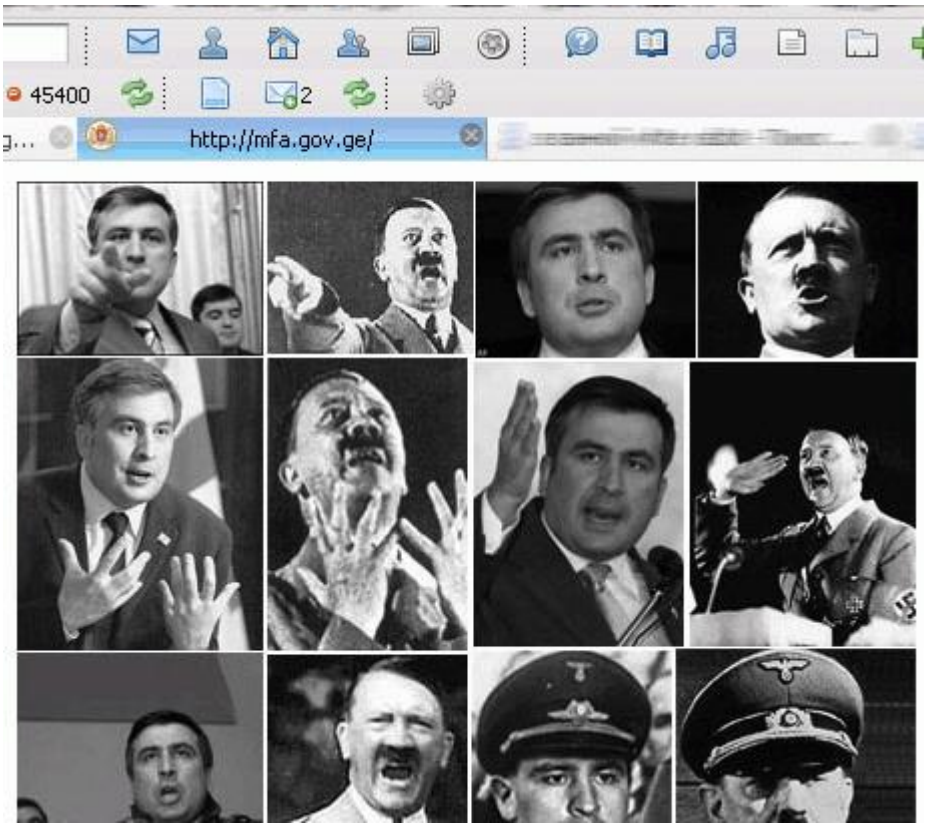

FIGURA 3: Captura de pantalla del sitio web del Presidente Saakashvili, tomada el 12 de agosto de 2008 (Cluley, 2008).

- Redirección de Tráfico

  Este tipo de ataque consiste en el enrutamiento del tráfico de datos del oponente a través de servidores propios o bajo control propio (US Joint Chief of Staff, 2013). Hay evidencias claras que indican que gran parte del tráfico de internet de Georgia fue redireccionado a través de servidores controlados por firmas de telecomunicaciones rusas. Investigadores informáticos de los Estados Unidos detectaron miles de redes infectadas con botnets[1] que generaban secuencias interminables de tráfico inútil hacia sitios web de Georgia. Estos programas maliciosos tenían la firma digital característica de grupos delictivos organizados para realizar estafas web, siendo el más conocido de ellos el grupo basado en San Petersburgo y conocido como RBN (Markoff, 2008).

El RBN[2] es un grupo delictivo organizado cuyas actividades se han centrado en la web, siendo responsable de robo de identidad, robo de datos, pornografía infantil y extorsión. Varios miles de páginas web rusas son propiedad de este grupo, sin que exista una identidad legal clara. El gobierno ruso no ha intentado detener las actividades de este grupo desde agosto de 2008, cuando cesaron todas las investigaciones. Otro de los sitios donde los hackers rusos coordinaban sus esfuerzos era stopgeorgia.ru, este sitio se encontraba alojado en servidores desde donde se han realizado fraude de pasaportes y estafas con tarjetas de crédito (AFCEA International, 2012).

En el año 2007, el periódico australiano The Age publicaba un artículo en el que relata los esfuerzos internacionales que se estaban realizando para poder llevar a juicio al grupo de cibercriminales conocidos como RBN. En el mismo artículo se cita que el líder del movimiento ruso, solo conocido por su apodo *Flyman*, es un familiar directo de "un prominente político ruso". El grupo RBN dejó de operar en 2006 en forma centralizada, es

[1] Se conoce con esta denominación a redes de computadores controladas en forma remota mediante código malicioso introducido en una o varias de las computadoras integrantes de dicha red. Se utilizan para generar volumen de tráfico en la web desde redes que no comprometen a los responsables del ataque.
[2] RBN: Russian Business Network

decir, desde servidores propios, atomizando sus operaciones desde millones de computadoras infectadas. En ese año, uno antes de la guerra entre Rusia y Georgia, se detectó que la mayoría de las redes que podía controlar este grupo criminal, se encontraban en los Estados Unidos y Europa Occidental, los mismos lugares desde donde, un año después, provendrían los pedidos de conexión que saturarían los servidores georgianos (Warren, 2007).

Si bien los ataques pueden no haber sido ejecutados en forma directa por fuerzas militares rusas, existen evidencias que en el pasado Rusia ha sido capaz de organizar los esfuerzos de hackers civiles. En numerosos sitios web rusos[3] o ubicados físicamente en servidores bajo control ruso se encontraban las herramientas y las instrucciones para que cualquier interesado pudiese colaborar con el ataque cibernético, sumando masa crítica a los ataques de denegación de servicio. Al pie de cada noticia publicada en sitios informativos rusos, en la sección de comentarios de lectores, podía encontrarse el código script para ejecutar ataques. Este script era posteado por hackers rusos en forma de comentario de la noticia publicada (Donovan, 2009).

Además de los ataques a los sitios web mediante las tres técnicas detalladas anteriormente, los ataques a la estructura de información también tuvieron su apoyo físico, mediante la destrucción de los nodos de subida y bajada de datos a los satélites de telecomunicaciones. El gobierno georgiano estaba, desde el punto de vista de la información, absolutamente bloqueado (Donovan, 2009).

1.2.3. Reacción de Georgia

Las capacidades de ciberdefensa de Georgia eran muy limitadas y fueron rápidamente sobrepasadas. La primera respuesta a los requerimientos masivos que generaba del ataque de DDOS[4] fue implementar filtros que impidieran el acceso desde servidores ubicados en Rusia. Esta acción no fue efectiva, ya que los hackers rusos la habían previsto y si bien los

[3] Consideramos sitios rusos a aquellos cuyo sufijo geográfico es .ru, independientemente de donde estén ubicados geográficamente.
[4] Denegación de Servicio Distribuido

ataques iniciales provenían mayoritariamente de servidores rusos, rápidamente activaron aquellas redes cuyo control habían adquirido previamente, pero que no habían sido utilizadas aún. Estas redes estaban, mayoritariamente, localizadas en Estados Unidos y Europa, como ya había anticipado Peter Warren un año antes. Los especialistas de ciberdefensa de Georgia se pusieron en contacto con sus pares de Estonia, con la intención de aprovechar la experiencia que estos habían adquirido el año anterior, durante los ciberataques rusos del incidente del Soldado de Bronce de Tallinn. Estonia compartió mucha de su experiencia e incluso envió expertos, pero no pudieron mitigar las acciones rusas, sino tan solo efectuar control de daños (AFCEA International, 2012).

La única medida efectiva que los georgianos pudieron implementar fue el traslado de sus sitios web esenciales a servidores en el extranjero. El sitio del Presidente Saakashvili mudó su host al servicio Google Blogs, el Ministerio de Defensa a un servidor privado en Atlanta, el Ministerio de Asuntos Exteriores a Estonia y la Oficina del Presidente de Polonia permitió que el gobierno de Georgia utilizara su página web para transmitir algunos mensajes oficiales (AFCEA International, 2012).

1.2.4. Organización de las fuerzas rusas

Durante todo el desarrollo del conflicto, las fuerzas rusas estuvieron bajo un comando unificado, a cargo de un General del Ejército Ruso. Este comando incluía a las fuerzas terrestres, navales y aéreas y a representantes de agencias gubernamentales cuyas tareas eran relevantes para el desarrollo de las acciones bélicas (Donovan, 2009).

Dado que Rusia niega su participación en los ataques cibernéticos, no hay evidencia que permita dilucidar si los ejecutores de los ciberataques estaban encuadrados dentro de las fuerzas asignadas al Teatro de Operaciones. Análisis efectuados por expertos en ciberseguridad de varios países indican que los hackers estaban fuera del control del Comandante del Teatro de Operaciones y bajo control directo de alguna agencia dependiente directamente del Gobierno de Moscú (Donovan, 2009).

La simultaneidad de las acciones cibernéticas y militares y la unidad de objetivo entre ambas es indicador suficiente de que, a pesar de la ejecución descentralizada de los ciberataques, su planeamiento tiene que haber sido centralizado. Como ya hemos expuesto, las herramientas y las instrucciones para participar del esfuerzo por saturar los sistemas web de Georgia estaban a disposición de cualquier persona que contase con una computadora y una conexión a internet (AFCEA International, 2012).

1.3. Lecciones del Conflicto

Dentro de los ataques cibernéticos sufridos por Georgia se pueden distinguir dos tipos distintos. Los ataques destinados a diseminar propaganda contra el gobierno de Georgia y los ataques contra la estructura de obtención y diseminación de información de Georgia.

1.3.1. Legitimidad de las Acciones Armadas

Los ataques de propaganda estuvieron destinados a evitar que Georgia pudiese reclamar la legitimidad de las acciones propias.

La Carta de las Naciones Unidas, en su artículo 2.4 prohíbe el uso de la fuerza contra la integridad territorial o la independencia política de un estado, por parte de cualquier otro estado. Existen, sin embargo, dos situaciones en que el uso de la fuerza se encuentra permitido, ellas son la Seguridad Colectiva y la Legítima Defensa. La primera depende exclusivamente de una resolución del Consejo de Seguridad de las Naciones Unidas (CSNU) y la segunda depende de que el estado agresor pueda probar que ha sido agredido y que ha actuado dentro de los límites del derecho internacional. Estar encuadrado dentro de una de estas dos situaciones es afirmar que las acciones son legítimas (Rodriguez Carrión, 2002).

Obtener la legitimidad de las acciones propias o negar la obtención de la legitimidad de sus acciones al enemigo es objeto de grandes esfuerzos durante todo el desarrollo del conflicto e incluso una vez que estos han finalizado. La obtención y mantenimiento de la legitimidad de las acciones propias puede conformar una Línea de Operaciones en sí misma, normalmente apoyada en el esfuerzo diplomático.

Los ciberataques que Georgia sufrió en sus sistemas cibernéticos impidieron no solo las operaciones bancarias y el comercio o el control de cuando y como se propagaban las noticias del conflicto, sino que, mediante la implantación de información en los servidores georgianos, se llegó a que los mismos ciudadanos e incluso los militares de Georgia dudaran de la legitimidad de las acciones propias. Una encuesta que la CNN realizó el 13 de agosto de 2008 pedía a los televidentes expresarse sobre su acuerdo o desacuerdo en referencia a la invasión rusa de Osetia del Sur. El 92% de los televidentes que participaron de la encuesta manifestó estar de acuerdo con las acciones rusas (Levine, 2008).

Rusia tampoco pudo lograr la legitimidad en el conflicto. Si bien el pueblo ruso apoyó el accionar militar de sus fuerzas en Georgia y los países regionales se abstuvieron de apoyar una clara invasión militar, las naciones de Europa Occidental y Estados Unidos no terminaron de creer que las acciones rusas fueran originadas por motivos de imposición de la paz o de asistencia a sus ciudadanos en Georgia. La creencia generalizada en estos países es que Rusia actuó principalmente para proteger su papel de distribuidor de energía a Europa, puesto que venía siendo desafiado por Georgia como centro de distribución de gas natural a mejores precios. Aun cuando los gasoductos rusos son más costosos que los ucranianos y georgianos, siguen siendo preferidos por las empresas energéticas europeas, dada la manifiesta capacidad y voluntad de Rusia de defenderlos (Donovan, 2009).

Quién estuvo detrás de estos ataques, sigue sin estar claro. Georgia explícitamente atribuye la responsabilidad a Rusia. Rusia siempre ha manifestado no haber participado en forma alguna de ataques informáticos a ninguna nación extranjera. Georgia, con una población de 4 millones de personas y con una estructura de información incipiente no sufrió ningún daño que se extendiera en el tiempo. Sin embargo, el gobierno georgiano estuvo totalmente imposibilitado de difundir su propio mensaje a sus ciudadanos o a los gobiernos de otras naciones. En ese momento Georgia estaba en el puesto 74 (de un total de 234) de las naciones con mayor cantidad de sitios de internet, detrás de Nigeria,

Bangladesh y Bolivia. Los ataques cibernéticos que sufrieron tuvieron un impacto comparativamente menor que el que hubiesen tenido en un estado que fuese más dependiente del uso de internet como Israel, Estados Unidos o las naciones de Europa Occidental (Markoff, 2008).

1.3.2. Análisis Doctrinario

Los ataques contra la estructura de información del gobierno georgiano y sus agencias y fuerzas armadas, así como varias organizaciones privadas, tuvieron por objetivo la afectación de los procesos de obtención y diseminación de información.

Las Operaciones de Información, en su aspecto ofensivo, tienen como propósito negar el uso, degradar o destruir la información almacenada en las redes de información del oponente (US Department of Defense, 2014).

Si revisamos los resultados de los ciberataques, observamos que estos efectos fueron cumplidos con éxito. Las noticias, los bancos, el comercio electrónico estuvieron detenidos en su mayoría o seriamente comprometido en algunos casos. Es por esto que, a pesar que se duda quienes fueron los que efectivamente realizaron las operaciones, no hay duda alguna que lo realizado en forma simultánea con una maniobra ofensiva terrestre fue una serie de operaciones cibernéticas ofensivas (AFCEA International, 2012).

1.3.3. Consecuencias en las fuerzas militares

En el plano estrictamente militar, no existen evidencias concretas que los ciberataques hayan disminuido la capacidad combativa de las unidades militares del Ejército Georgiano. Los ciberataques no incluyeron la intrusión en sistemas estrictamente militares, sino que pusieron énfasis como se ha descripto, en sitios públicos y en la infraestructura virtual de comercio, bancos y noticias. La intención principal de los ciberataques fue aislar al gobierno georgiano de los medios de comunicación, de forma de no permitir que sus mensajes fueran diseminados. Aunque no hay registros de ataques sobre los sistemas de información, la efectiva distribución de propaganda generó que un número significativo de miembros de las tropas georgianas presentaran dudas en cuanto a la

legitimidad de las órdenes recibidas. Además de la comparación del Presidente Saakashvili con dictadores, se distribuyeron informes que consignaban que la finalidad del conflicto no era otra que resguardar inversiones personales en Osetia del Sur (Donovan, 2009).

Las fuerzas rusas se encontraban desplegadas en la zona fronteriza desde inicios de inicios del mes de julio, realizando diversos ejercicios militares. Aún después que los ejercicios terminaron, las tropas permanecieron en estado de alerta. Es decir que, al momento de entrar en Osetia del Sur el 8 de agosto, las tropas rusas cumplían con casi 40 días de despliegue operativo, en un estado permanente de máxima alerta, lo que conlleva un desgaste psicofísico importante. Sin embargo, las tropas rusas ingresaron en Osetia del Sur y en una semana demostraron una superioridad abrumadora sobre las fuerzas georgianas, degradando seriamente su capacidad efectiva de largo plazo. Los efectos observados sobre ambos ejércitos son similares en naturaleza, pero opuestos en su aplicación. La fricción en el ejército de Georgia aumentó, demorando decisiones y generando malestar entre las tropas. En el ejército de Rusia infundió un sentimiento de causa justa, que tuvo un efecto contrario al sufrido por los georgianos (AFCEA International, 2012).

CAPÍTULO 2: DESCENTRALIZACIÓN DE LAS CIBEROPERACIONES

2. DESCENTRALIZACIÓN DE LAS CIBEROPERACIONES

2.1. Ciberoperaciones

Definiremos Ciberespacio como el dominio que se caracteriza por el uso de la electrónica y el espectro electromagnético para almacenar, modificar e intercambiar datos a través de sistemas en redes y su infraestructura física asociada (US Joint Chief of Staff, 2011).

Cuando una organización militar se despliega en el teatro de operaciones y conecta sus sistemas en red, se crea un ciberespacio, independientemente que dicha red se encuentre conectada externamente a cualquier otra red militar, regional o la internet misma. Dicho ciberespacio debe ser controlado, protegido y de encontrar el del oponente, explotado (Williams, 2014).

Gran parte de las operaciones militares actuales requieren del uso del ciberespacio. Los desarrollos en este campo permiten a las fuerzas militares obtener y mantener la ventaja en el ambiente operacional. Esto presenta una paradoja, ya que este ambiente donde se despliegan herramientas que nos permiten mantener la iniciativa contra el oponente, es también un espacio de interés para que los mismos oponentes actúen sobre nuestras fuerzas o sistemas de comando y control. O sea que un sistema que nos proporciona una ventaja, nos genera debilidades que debemos proteger de la explotación del oponente (US Joint Chief of Staff, 2013).

Actualmente el Departamento de Defensa de los Estados Unidos, en su publicación doctrinaria conjunta *"Cyberspace Operations"* clasifica las ciberoperaciones en:

- Operaciones de Redes de Información

  Las Redes de Información son todos los sistemas desplegados que se utilizan para la obtención, diseminación y proceso de la información entre todos sus nodos. Las operaciones que se ejecutan para instalar, operar, mantener y

proteger dichas redes son operaciones de redes de información (Williams, 2014).

- Ciberoperaciones Defensivas.
  Son aquellas operaciones desarrolladas en forma pasiva o activa, en el ciberespacio o a través de él, que impidan al oponente contar con una ventaja sobre los sistemas propios y si la ha adquirido, desarticularla. Nótese que esta definición contempla el concepto de defensa ofensiva (Williams, 2014).

- Ciberoperaciones Ofensivas.
  Aquí se encuadran las operaciones que se ejecutan en o a través del ciberespacio para proyectar poder mediante la aplicación de una fuerza.

2.2. Ciberoperaciones en el Nivel Operacional

En el año 2009 el Secretario de Defensa de los Estados Unidos creó el Ciber Comando de los Estados Unidos (USCYBERCOM), a la luz de las lecciones aprendidas principalmente en:

- Los ciberataques de Estonia de 2007.
- Los ciberataques de Georgia de 2008.
- Los ciberataques, de supuesto origen chino ocurridos entre 2003 y 2005, conocidos como “Titan Rain”.

El USCYBERCOM es un comando dependiente del Comando Estratégico de los Estados Unidos y entre varias tareas, controla los cuatro subagencias pertenecientes al ejército, la armada, la fuerza aérea y la infantería de marina. Estas están formadas con personal propio de cada fuerza, adiestrado especialmente en la planificación y/o ejecución de ciberoperaciones. Para cada una de las fuerzas, estas unidades (que poseen una estructura cuasi regimental) poseen entre 500 y 1000 efectivos y realizan todo tipo de ciberoperaciones, defensivas, ofensivas y de redes información (Fitzgerald & Wright, 2014).

Desde el año 2009, el USCYBERCOM ha desplegado más de cien equipos con el objetivo de defender infraestructuras de información críticas y proteger redes de información. Cada vez que la tarea de estos equipos ha debido extenderse fuera

de los límites geográficos de los Estados Unidos, el control ha recaído en alguno de los Comandos Combatientes Unificados[5] (Fitzgerald & Wright, 2014).

Estos comandos unificados, desarrollan sus actividades en el nivel operacional, con muchas similitudes al comando de un teatro de operaciones, pero sin ser exactamente lo mismo.

Estos Comandantes Combatientes reconocen a los equipos de ciberoperaciones que se les asignan como un integrante de su poder de combate y les asignan tareas que permite proyectar poder con bajo riesgo operacional y de detección y le permite utilizar fuerzas para otras tareas que los equipos pueden cubrir como ISR[6]

El General Brett Williams, Director de Operaciones del USCYBERCOM hasta su retiro en 2014, en su trabajo *"The Joint Force Commander Guide to Cyberspace Operations"* establece cuatro axiomas que permiten entender porque él sostiene que debe descentralizarse el planeamiento y la ejecución de las ciberoperaciones.

1. *El uso de la palabra ciberguerra no es productivo.*
   El ciberespacio no es una nueva forma de guerra. El ciberespacio es solo un nuevo dominio donde la guerra puede ser conducida. Las ciberoperaciones no cambian la naturaleza de la guerra, de la misma forma que no lo hizo la introducción de las aeronaves. No existe la ciberguerra, sino las ciberoperaciones.

2. *La doctrina conjunta existente enmarca perfectamente a las ciberoperaciones.*
   El modelo de planificación conjunta que conocemos con la denominación de Diseño Operacional es perfectamente capaz de contener y enmarcar la planificación de ciberoperaciones como una línea de operaciones en apoyo o apoyada por otras similares. No es necesario deducir nuevos procedimientos.

3. *Los operadores deben ser militares con formación en Operaciones y Planes.*

[5] Comandos con asignación territorial y de fuerzas militares de, al menos, dos fuerzas armadas distintas. Estos son USAFRICOM, USCENTCOM, USNORTHCOM, USSOUTHCOM, USPACOM Y USEUCOM.
[6] Intelligence, Surveillance and Reconoissance – Inteligencia, Vigilancia y Reconocimiento

Existe una tendencia a dotar a las organizaciones de ciberoperaciones de personal técnico, especialmente provenientes de Comunicaciones, Inteligencia y Criptología, disciplinas más caracterizadas como de apoyo. Más allá de la aparente necesidad de satisfacer los requerimientos técnicos que este tipo de operaciones posee, se debe tener en cuenta que, al igual que en cualquier otro tipo de esfuerzo operacional, el éxito se garantiza con planeamiento y liderazgo

4. *No utilizar el prefijo ciber en todos los términos militares.*

   El mal uso, rutinario y sostenido, del prefijo ciber es la principal causa que se haya tardado tiempo en encontrar un marco de referencia común a todas las fuerzas en este aspecto. El mal uso de términos como ciberinteligencia o cibercomunicaciones, entre muchos otros, ha logrado confundir a quienes han intentado adaptar los procedimientos existentes a este tipo de operaciones.

2.3. Integración de las Ciberoperaciones con la Maniobra Operacional

La Maniobra, como Principio de la Guerra se define como la aplicación flexible del poder de combate para colocar al oponente en una situación de desventaja. La Maniobra Operacional, a su vez, es una combinación de movimientos y efectos, secuenciales y/o simultáneos que se desarrollan en un Teatro de Operaciones para alcanzar un Objetivo Operacional (Estado Mayor Conjunto de las Fuerzas Armadas Argentinas, 2015).

La maniobra en una ciberoperación es la aplicación de fuerza para capturar, interrumpir, negar, degradar, destruir o manipular los recursos de información y computación del oponente, para obtener una posición relativa ventajosa. En los dominios tradicionales de la guerra, la maniobra implica el posicionamiento de fuerzas militares. En el ciberespacio, en cambio, no hay movimientos, en el sentido cinético de masas desplazándose o realizando acciones físicas sobre objetivos materiales. En el ciberespacio la fuerza no son los operadores de los sistemas de información o de comando y control, la fuerza es el código utilizado para cumplir un objetivo en los sistemas del oponente o para proteger los propios. Conceptualmente, en el ciberespacio no son las fuerzas las que se mueven, sino los puntos desde donde los ataque se originan. El caso de la guerra entre Rusia y Georgia es ejemplo claro de esto, la mayoría de las redes desde

donde provenían las solicitudes que conformaron el ataque de denegación de servicio distribuido, fue de Estados Unidos, no desde Rusia, donde se encontraban los operadores de los botnet (Applegate, 2012).

Esto presenta, aparentemente, el primer problema para encuadrar una acción en el ciberespacio en el nivel operacional. El campo de acción del nivel operacional es acotado geográficamente. La autoridad investida a un Comandante del Teatro de Operaciones (CTO) es otorgada con límites geográficos bien definidos ya que la misma autoridad que designa al comandante, también establece taxativamente el Teatro de Operaciones (TO) (Estado Mayor Conjunto de las Fuerzas Armadas Argentinas, 2015).

La contribución académica "Arte y Diseño Operacional" define a un Teatro de Operaciones como *un área geográfica terrestre, marítima o mixta y el aeroespacio asociado, establecida por la máxima autoridad nacional, para la conducción de operaciones militares, a cargo de un Comandante del Teatro de Operaciones* (Kenny, Locatelli, & Zarza, 2015).

En el ciberespacio no hay límites físicos claros, como los hay en los otros dominios de la guerra. El combatiente terrestre conoce su ubicación y la de su objetivo, pero el operador de sistemas de información puede no saber cuál es la ubicación física exacta de su objetivo (o su agresor) y, sin embargo, puede accionar eficazmente contra sus intenciones. En el dominio físico de la guerra las operaciones son fácilmente caracterizables como regionales, zonales o globales. Esta clasificación en el ciberespacio no se aplica, al menos no fácilmente (Birdwell & Mills, 2011).

2.4. Comando y Control de Ciberoperaciones en el Nivel Operacional

Existen varios esquemas de Comando y Control que se utilizan en otros aspectos de la conducción de la guerra que pueden ser adaptados para encontrar la mejor estructura de comando y control para los equipos de ciberoperaciones.

En un lado del espectro tenemos el esquema que se utiliza más frecuentemente en el diseño de sistemas logísticos y en asignación de apoyos de fuego. Este es el concepto de Apoyo. Este tipo de asignación de fuerzas o esfuerzos establece que, si bien un comandante tiene prioridad de empleo para esa fuerza, no tiene

completo control sobre ella. En este esquema, los equipos de ciberoperaciones permanecen bajo el control del nivel estratégico militar, pero en apoyo del nivel operacional, es decir que el CTO planificará su operación y elevará los requerimientos al nivel estratégico militar, pero el planeamiento de las acciones de ciberoperaciones no dependerá de él. En el lado opuesto del espectro, el concepto de Agregación o Asignación, entrega el control total al CTO sobre los equipos de ciberoperaciones (Fitzgerald & Wright, 2014).

Si consideramos que ambos niveles, el estratégico militar y el operacional poseen necesidades reales de participar en el planeamiento y ejecución de las ciberoperaciones, surge un esquema que mezcla algunas características de los detallados previamente. En este esquema, el CTO mantiene el C*omando Operacional* sobre los equipos de ciberoperaciones que la estrategia militar le asigna y a su vez el CTO se encuentra bajo Control Operacional de la agencia de ciberoperaciones de la Estrategia Militar.

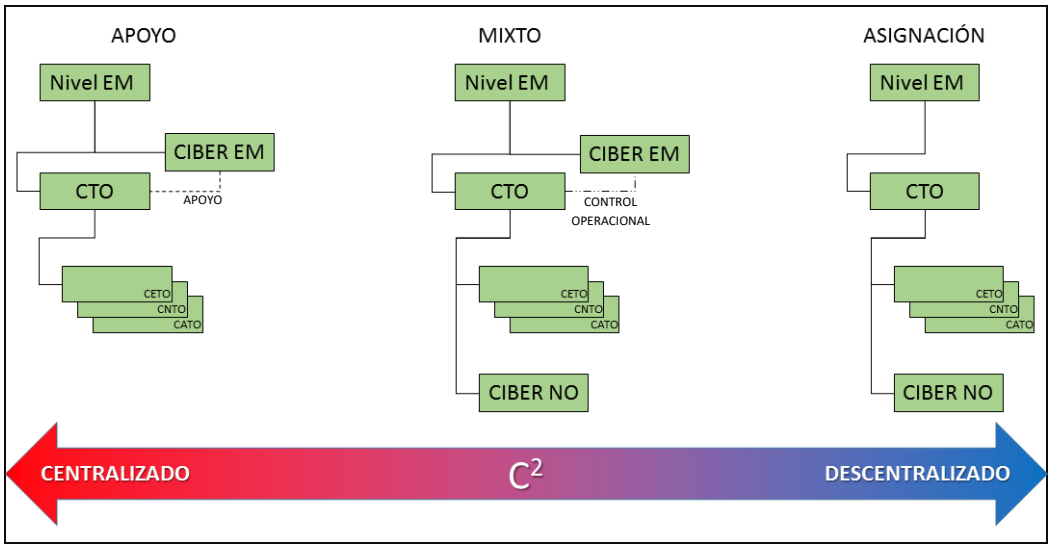

FIGURA 4: Estructuras de Comando y Control para equipos de ciberoperaciones en el Nivel Operacional

La Estrategia Militar debe encontrar un balance. establecer un esquema *de apoyo* y un esquema *de asignación*. En la Figura 4 podemos ver una representación gráfica de los tres esquemas descriptos anteriormente. El esquema de Apoyo es en el que el Nivel EM retiene toda la autoridad sobre los equipos de ciberoperaciones. En el Esquema de Asignación, esa autoridad la tiene el CTO. El esquema intermedio es el que ofrece compromiso entre la autoridad del CTO para

asignar tareas a sus equipos de ciberoperaciones y al Nivel EM de mantener las ciberoperaciones del TO dentro de las políticas establecidas por el Nivel Estratégico Nacional, a través de su propio organismo de ciberoperaciones (US Department of Defense, 2015).

Ninguna estructura de comando y control es perfecta. Además, el comando y control, por sí mismo, no asegura capacidades ni efectividad en el empleo de los medios para la concreción de los fines. Estas estructuras deben evolucionar en forma permanente en base a la experiencia directa y a la situación planteada por el ambiente y por el oponente. Esto es especialmente cierto para las estructuras de comando y control en ciberoperaciones, dado que es un ambiente de muy alto dinamismo (Fitzgerald & Wright, 2014).

CONCLUSIÓN FINAL

En 2008, las fuerzas terrestres rusas asestaron un golpe mortal a la capacidad de defensa de la República de Georgia y lo hicieron en apenas una semana de operaciones. Aún hoy, ocho años después del enfrentamiento, el Ejército de Georgia no ha recuperado su poder de combate.

El éxito en la campaña terrestre estuvo asegurado por varios aspectos, siendo el más importante de ellos que la distribución del poder de combate relativo era abrumadoramente favorable a las fuerzas rusas, que sumaban a milicianos osetios y abjasios, aun cuando no los necesitaban para el cumplimiento de sus objetivos.

Pero el éxito político de la campaña estuvo marcado por el hecho de que el Presidente Sakaashvili estuvo imposibilitado de manifestar la posición de Georgia. Los escasos comunicados que el gobierno de Tiflis pudo hacer llegar al resto del mundo estuvieron rodeados de una campaña de desinformación a través de internet, particularmente de sitios de noticias del propio país.

Si bien este esfuerzo fue suficiente para que Georgia no pudiese declararse como estado agredido, tampoco fue suficiente para que Rusia estableciera, sin lugar a dudas, que había actuado en defensa de sus propios ciudadanos. Esto fue porque los análisis de tráfico y auditorías de redes que se realizaron con posterioridad a las acciones bélicas arrojaron que la campaña de desinformación se había originado en redes que, ya se sabía, estaban captadas por rusos. Más exactamente, por criminales rusos supuestamente alineados con el gobierno de Medvedev y Putin. Esto dio por el suelo con las aspiraciones rusas de obtener plena legitimidad por sus acciones.

El Comandante del Teatro de Operaciones Georgia consiguió el efecto deseado, combatiendo sobre territorio del enemigo y dañando seriamente la capacidad de estos de responder en el futuro, pero no tuvo control sobre una de las líneas de esfuerzo del plan general, la correspondiente a ciberoperaciones.

Otro aspecto a considerar del caso de estudio es la capacidad de movilización ciudadana que generó el impacto de los primeros ciberataques. Durante el Conflicto del Atlántico Sur, la movilización de personal al TOAS estuvo limitada por capacidades de carga, pesos y otros factores logísticos. En este conflicto, las herramientas para participar del conflicto estaban disponibles en el dominio público, lo que sumó centenares de activistas que

contribuyeron al esfuerzo sin necesidad de desplazarse, ni consumir recursos del esfuerzo militar.

Por otro lado, hemos establecido la dependencia que la economía en general y las fuerzas militares en particular, tienen hoy de los sistemas de información. Estados Unidos, uno de los pocos países del mundo con un despliegue global verdadero ha iniciado un proceso de cesión de atribuciones del nivel estratégico militar de planeamiento y ejecución de ciberoperaciones, al nivel operacional.

Si bien este es un proceso en desarrollo, los trabajos consultados inician en el año 2014, los primeros resultados han sido satisfactorios y, como principal enseñanza, para el planeamiento y ejecución de las ciberoperaciones se ha utilizado el método preexistente de planeamiento, el del Diseño Operacional.

Procesos similares han sido iniciados por el Reino Unido y Canadá que no han sido tratados en este trabajo por una cuestión de espacio y porque la solución a la que arribaron es similar (Chief of the Defence Staff , 2014) (Bernier & Treurniet, 2009).

BIBLIOGRAFÍA

Acosta, O. P. (2013). *Capacidades para la Defensa en el Ciberespacio.* Madrid: Isdefe.

AFCEA International. (2012). *The Russo-Georgian War 2008: The Role of the Cyber Attacks in the Conflict.* AFCEA International.

AFP. (10 de agosto de 2008). *LaNacion.com*. Recuperado el 23 de septiembre de 2016, de Los puntos calientes en el polvorín del Cáucaso: http://www.nacion.com/mundo/puntos-calientes-polvorin-Caucaso_0_993900697.html

Applegate, S. D. (2012). The Principle of Maneuver in Cyber Operations. Fairfax: George Mason University.

Ashmore, W. C. (2009). *Impact of Alleged Russian Cyber Attacks.*

Bank of England. (25 de junio de 2014). *Consolidated Statements 2014*. Recuperado el 23 de mayo de 2016, de http://www.bankofengland.co.uk/publications/Documents/bankreturn/2014/140625cs.pdf

Bell, D. (1999). *The Coming of Post Industrial Society.* New York: Basic Books.

Bernier, M., & Treurniet, J. (2009). *Canadian Forces Cyber Operations in the Future Cyber Environment Concept.* Ottawa: Defence and Research and Development Canada.

Bernier, M., & Treurniet, J. (2010). *Understanding Cyber Operations in a Canadian Strategic Context: More than C4ISR, More than CNO.* Tallinn: Defence Research and Development Canada.

Birdwell, B., & Mills, R. (2011). La Conducción de la Guerra en el Ciberespacio. *Air & Space Power Journal*, 23-35.

Cahanin, S. E. (2012). Principios Bélicos del Ciberespacio. *Air Space Power Journal en español, XXIII*(3), 73-82.

Chang, W., & Granger, S. (2012). La Guerra en el Ámbito Cibernético. *Air & Space Power Journal en español, XXIII*(3), 83-90.

Chief of the Defence Staff . (2014). *UK Defence Doctrine.* Londres: UK Chiefs of Staff.

Cluley, G. (12 de agosto de 2008). *naked security by Sophos*. Recuperado el 11 de octubre de 2016, de Conflict Between Russia and Georgia Turns to Cyber Warfare: https://nakedsecurity.sophos.com/2008/08/12/conflict-between-russia-and-georgia-turns-to-cyber-warfare/

Cronin, A. K. (enero de 2006). Cyber-Mobilization: The New Levée en Masse. *Parameters, 36*(2), 77-87.

Donovan, G. T. (2009). *Russian Operational Art in the Russo-Georgian War of 2008.* Carlisle Barracks: US Army War College.

Ducheine, P., & van Haaster, J. (2014). Fighting Power, Targeting and Cyber Operations. *6th International Conference on Cyber Confl ict* (pág. 25). Tallinn: Nato CCDCOE.

Estado Mayor Conjunto de las Fuerzas Armadas Argentinas. (2015). *Planeamiento para la Acción Militar Conjunta - Nivel Operacional.* Buenos Aires: EMCFFAA.

Estado Mayor de la Defensa. (2009). *Doctrina para la Acción Conjunta de las Fuerzas Armadas.* Madrid: Ministerio de Defensa Español.

Estonian Republic Statistics Center. (14 de enero de 2016). *Estonian Republic Statistics Center*. Recuperado el 23 de mayo de 2016, de http://www.staat.ee/34278

European Parliament. (2014). *Cyber Defence in the EU: Preparing for Cyber Warfare?* Bruselas.

Fitzgerald, B., & Wright, P. (2014). *Digital Theaters: Decentralizing Cyber Command and Control.* Washington DC: Center for a New American Security.

George, J. (2009). *The Politics of Ethnic Separatism in Russia and Georgia.* New York: Palgrave McMillian.

Giudici, C. A. (2013). *Lineamientos para la Seguridad Cibernética en un Teatro de Operaciones.* Buenos Aires: Escuela de Guerra Conjunta.

Gómez Arriagada, H. (2013). Ciberoperaciones. *Revista de Marina*, 362-367.

Hunker, J. (2010). *Cyber war and cyber power: Issues for NATO doctrine.* Roma: NATO Defense College.

Jefatura de Gabinete de Ministros. (2005). *Modelo de Política de Seguridad de la Información para Organismos de la Administración Pública Nacional.* Ciudad Autónoma de Buenos Aires.

Joint Chief of Staff. (2013). *Cyberspace Operations.* Washington DC.

Kenny, A., Locatelli, O., & Zarza, L. (2015). *Arte y Diseño Operacional.* Buenos Aires: Escuela Superior de Guerra Conjunta de las Fuerzas Armadas.

Levine, Y. (13 de agosto de 2008). *The Exiled*. Recuperado el 13 de octubre de 2016, de The CNN Effect: Georgia Schools Russia in Information Warfare: http://exiledonline.com/the-cnn-effect-georgia-schools-russia-in-information-warfare/

Lewis, J. A. (2015). *The Role of Offensive Cyber Operations in NATO´s Collective Defence.* Tallinn: NATO Cooperative Cyber Defence Center of Excellence.

Lewis, J., & Timlin, K. (2011). *Cybersecurity and Cyberwarfare.* Ginebra: Center for Strategic and International Studies.

Libicki, M. C. (2009). *Cyberdeterrence and Cyberwar.* Arlington: Rand Project Air Force.

Markoff, J. (12 de Agosto de 2008). Before the Gunfire, Cyberattacks. *The New York Times*.

Ministerio de Defensa. (2015). *Decisión Administrativa 15/2015.* Ciudad Autónoma de Buenos Aires.

Paez, E. P. (2014). *La Guerra Cibernética en el Nivel Operacional.* Buenos Aires: Escuela de Guerra Conjunta.

Rehman, S. (23 de mayo de 2016). *Estonia's Lessons in Cyber Warfare*. Obtenido de US News - World Report: http://www.usnews.com/opinion/blogs/world-report/2013/01/14/estonia-shows-how-to-build-a-defense-against-cyberwarfare

Richards, J. (31 de agosto de 2016). *International Affairs Review*. Obtenido de http://www.iar-gwu.org/node/65

Rivolta, A. S. (2012). *Las Vulnerabilidades de las Operaciones Militares Derivadas de las Redes Sociales en Internet.* Buenos Aires: Escuela de Guerra Conjunta.

Rodriguez Carrión, A. J. (2002). *Lecciones de Derecho Internacional Público.* Madrid: Tecnos.

Rodriguez Cisneros, E. (2012). *Desafíos Operacionales en el Ciberespacio Como Nuevo Campo de Lucha.* Buenos Aires: Escuela de Guerra Conjunta.

Rojo, J. (2013). *Los elementos del Diseño Operacional en la Guerra Ruso Georgiana del Año 2008.* Buenos Aires: Escuela de Guerra Conjunta.

The Christian Science Monitor. (19 de agosto de 2008). *The Christian Science Monitor*. Recuperado el 2 de septiembre de 2016, de http://www.csmonitor.com/World/Europe/2008/0819/p12s01-woeu.html

Thomas, T. (enero de 2015). Russia´s 21st Century Information War. (NATO, Ed.) *Defence Strategic Comunications, 1*(1), 11-26.

US Air Force. (2010). *Air Force Cyberspace Operations.* Washington DC: US Air Force.

US Central Intelligence Agency. (13 de octubre de 2016). *The World Factbook*. Recuperado el 18 de octubre de 2016, de https://www.cia.gov/library/publications/the-world-factbook/geos/en.html

US Department of Defense. (20 de noviembre de 2014). *Defense Technical Information Center*. Recuperado el 8 de septiembre de 2016, de http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf

US Department of Defense. (2015). *The DoD Cyber Strategy.* Washington DC: US DoD.

US Joint Chief of Staff. (2011). *Joint Terminology for Cyberspace Operations.* Washington DC.

US Joint Chief of Staff. (2013). *JP 3-12 (R) Cyberspace Operations.* Washington DC.

Vice Chairman of the Joint Chiefs of Staff. (2012). *Joint Terminology for Cyberspace Operations.* Washington DC: Joint Chiefs of Staff.

Warren, P. (13 de diciembre de 2007). *The Hunt for Rusia´s Web Crimes*. Recuperado el 3 de octubre de 2016, de The Age: http://www.theage.com.au/news/security/the-hunt-for-russias-web-crims/2007/12/12/1197135470386.html

Williams, B. T. (2014). The Joint Force Commander's Guide to Cyberspace Operations. *Joint Force Quarterly #73*, 12-19.

Ziegler, C. (2011). *Russia, Central Asia and the Caucasus after the Georgia Conflict.* New York: Palgrave McMillian.

COPIA DIGITAL DEL TRABAJO FINAL INTEGRADOR
CONTIENE:

- Trabajo Final Integrador
- Bibliografía Digital Parcial