Ciberguerra - Nuevas formas de hacer la guerra en el siglo XXI

"Cien victorias en cien batallas no es lo ideal, lo ideal es someter al enemigo sin luchar"
(Sun tzu, 600 años a.c).

Teniente Coronel Luis Martín Moreno
Miembro del equipo de investigación del Departamento Ejército

Foto: http://oronegro.mx/2016/05/04/anonymous-declara-la-guerra-a-bancos-del-mundo/

Resumen.

En la era de la información[1] intervienen un conjunto de sistemas de información y comunicaciones[2] en un proceso articulado a partir de la recolección de datos por sensores satelitales, aeronaves, el monitoreo y sistemas de cómputo y vigilancia. En medio de este complejo tecnológico, se abre paso el nuevo campo del combate virtual, ya no como aquella extensión de espacio propicia para enfrentar al enemigo con determinada cantidad de tropa, equipo y capacidades suficientes para tal fin. Ahora, se presenta como un territorio de carácter virtual.

Palabras clave: Guerra virtual; Ciberataques; Conflictos modernos.

El ciberespacio es el campo de batalla del pelotón de avanzada de países desarrollados, donde las municiones son unos y ceros (Huerta, 2015, párr. 1). Por ende, el enemigo no tendría necesidad de innovadores sistemas de armas y tecnologías de punta para suponer una amenaza a cualquier Estado. Este trabajo de investigación tiene el propósito de abordar los efectos de la ciberguerra en los conflictos modernos. El presente artículo argumenta que la ciberguerra se considera como una amenaza real a la seguridad nacional en Colombia. Esto, por la dinámica adquirida por las tecnologías de la información y las comunicaciones en el mencionado campo virtual, así como por la incertidumbre sobre la responsabilidad penal del uso indebido del ciberespacio.

De este modo, las Tecnologías de la Información y las Comunicaciones (en adelante TIC´s) producen cambios revolucionarios [3] cuyo dinamismo genera vulnerabilidades en los sistemas en red, imponiendo un alto grado de demandas en seguridad por parte de los usuarios. El virtual, se convierte en el espacio ideal para la impunidad y el delito por las facilidades que este ofrece. La intangibilidad de la nueva dimensión permite la personificación de nuevas amenazas que terminaron por modificar a su vez el tradicional escenario de la defensa (Sáenz, 2012, p. 29).

Los riesgos de esta naturaleza, se materializan en ataques cibernéticos, produciendo daños potencialmente significativos a infraestructura clave, activos económicos del Estado y otros [4] que afectan la estabilidad nacional. Razón por la que la seguridad del ciberespacio es un compromiso mayor para la supervivencia del Estado. Según el Instituto Español de Estudios Estratégicos (2010), el ciberataque se define como una forma de ciberguerra, que combinada o no con ataques físicos, intenta acceder o impedir el uso de sistemas en red al adversario.

Antecedentes: Ciberataques y vulnerabilidad de la Seguridad Nacional.

Por tanto, la ciberguerra [5] se focaliza en el colapso del flujo de información tanto civil como militar, perturbando el normal funcionamiento del Estado[6] así como el desarrollo de las operaciones militares[7] obteniendo según Denning (2001) los mismos efectos estratégicos que una acción armada convencional. Al enunciar los casos más destacados desde finales del siglo XX hasta lo corrido del siglo XXI, se debe detallar la guerra de Yugoslavia en 1999, punto de partida para algunos autores. Estos coinciden en afirmar que allí se presentaron las primeras manifestaciones de ciberguerra, pues

1 Tecnologías en campos de la Informática y Comunicaciones alteraron el diario vivir de la vida humana, formas de comunicación, trabajo, educación, hasta tiempo libre, haciendo de la época una distinción a la del mundo contemporáneo conocida como la era de la información y las comunicaciones. Ver: *La paradoja del poder norteamericano de Nye J. Madrid:Taurus 2003*.

2 TIC. Tecnologías de Información y Comunicaciones refuerzan el ejercicio del mando, así como el control político y militar de las operaciones. Ver: *entre la revolución y la trasformación de Guillermo Colom Piella.*

3 Dichos cambios pueden trasformar las Fuerzas armadas, hasta el modo de hacer la guerra. Se recomienda ver: Revoluciones militares y Revoluciones en asuntos militares 1300-2050 de los historiadores estadunidenses Murray y Knox.

4 Penetración en la red de comunicación, mando y control de las Fuerzas Armadas.

5 Considerada como una nueva tipología del conflicto virtual, donde se introduce el concepto de guerra en red (NetWear) que puede adoptar actores no estatales que se organizan en redes para actuar. Se recomienda ver: In Athenea´s Camp: *Preparándose para la guerra de la información*, Santa Mónica, de Arquilla J. y Ronfeldt D.

6 Afecta movimientos financieros (colapso, paralización), alteración de datos de bases públicas o privadas, redes de información y comunicaciones, otros.

7 Entorpecimiento del mando y control.

ya se identifican algunas acciones como el bloqueo de las redes telefónicas de Yugoslavia por la Otan, un ciberataque por parte de *Hackers* chinos a las redes informáticas del Gobierno estadounidense[8] tras el bombardeo de la Embajada China en Belgrado, entre otros eventos.

Otros de mayor importancia previos al comienzo de la guerra convencional entre Georgia y Rusia en 2008 son los ciberataques denunciados en su momento por Georgia. Una serie de ataques masivos desde el ciberespacio en contra de sus sistemas de infraestructura crítica, medios de comunicación, la banca y el transporte fueron realizados por hackers rusos. Al igual, semanas antes de iniciar el conflicto, en julio de 2008, la página web del presidente georgiano fue bloqueada por un ataque cibernético. Además se ejecutó la desfiguración del sitio web, en el cual fotos de Hitler se pusieron al lado de las fotos del presidente del Estado, finalmente tales ciberataques acompañaron los ataques convencionales rusos (Cornell & Star, 2009).

Igualmente, en 2007 diversos sistemas de Estonia fueron afectados masivamente por un ataque de denegación de servicio como consecuencia de la decisión del gobierno de remover un monumento ruso que representaba para Rusia la liberación de Estonia, de Hitler. El mismo era percibido por Estonia como símbolo de represión por parte de Rusia. Las redes de Estonia fueron inundadas por datos procedentes de Rusia, sin embargo, probablemente no por el Estado, sino por organizaciones patrióticas.

En la ocasión, algunos equipos tuvieron un aumento de 1.000 solicitudes por día a 2.000 solicitudes por segundo y el ataque se prolongó durante semanas. Las páginas web del gobierno, los partidos y los bancos fueron atacados y se colapsaron. La agresión provocó que Estonia pidiera la intervención de la Otan y, en agosto del 2008, se puso en marcha el centro de Excelencia para la Cooperación en Ciberdefensa (CCD) de la Otan en Tallin, capital de Estonia.

Sin embargo, el hecho más relevante que destaca el daño a la infraestructura crítica, es el ataque a Irán con el virus *Stuxnet* en 2009-2010. Este

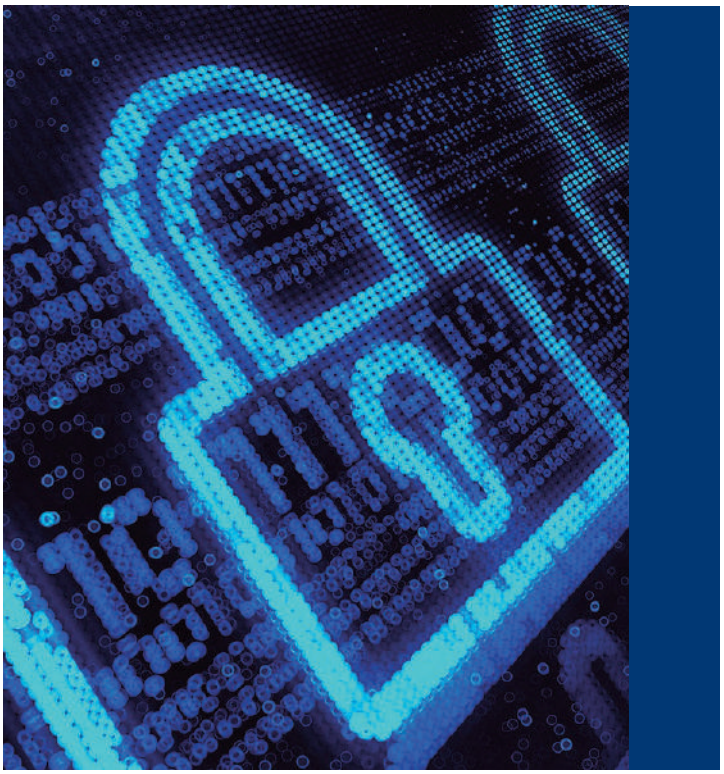

Foto: https://www.interempresas.net/Seguridad/Articulos/147749-Panda-Security-revela-ataques-ciberneticos-a-organismos-publicos-de-todo-el-mundo.html

fue el primer virus informático específicamente diseñado para causar daño en el mundo real, guiado por el mundo virtual. A diferencia de los casos anteriormente mencionados, este *malwere* es capaz de causar problemas físicos secundarios, afectando de manera específica el *software* que controla los sistemas industriales. Concretamente, *Stuxnet* fue diseñado para dañar la maquinaria en las instalaciones de enriquecimiento de uranio iraní en Natanz. Wilson, (2008).

De acuerdo con la BBC News (2010), la intrusión del virus *Stunext* en el sistema informático del reactor nuclear Busher desató la destrucción de un número importante de centrifugadoras de Irán, esencialmente lavadoras gigantes utilizadas para enriquecer uranio, haciéndolas girar fuera de control hasta autodestruirse.

"El virtual, se convierte en el espacio ideal para la impunidad y el delito por las facilidades que este ofrece".

8 Entre ellos el sitio WEB de la Casa Blanca permaneció fuera de servicio más de tres días.

"Una serie de ataques masivos desde el ciberespacio en contra de sus sistemas de infraestructura crítica, medios de comunicación, la banca y el transporte fueron realizados por hackers rusos".

Cabe señalar que *Stuxnet* es capaz de propagarse activamente a otros sistemas, explotando vulnerabilidades del sistema Windows, según *The Washintong* Post (2012) y considera que este nuevo prototipo de arma cibernética, es capaz de conducir a una nueva carrera armamentista. Se estima que durante el año 2009 antes de ser descubierto ya habría infectado los primeros computadores en Irán a través de una memoria USB infectada.

De esta forma, estos ataques cibernéticos dejan en evidencia la vulnerabilidad estratégica de los Estados a partir del ciberespacio. Pues bien, tales antecedentes han mostrado la magnitud del daño que se puede generar con el sabotaje a infraestructura crítica, paralización de redes de trasporte, interrupción de energía, ataques a reactores nucleares y otros. Todos ellos iniciados a partir de redes de internet.

Foto: http://www.ibtimes.co.uk/john-mcafee-few-us-will-survive-global-cyber-war-thats-looming-horizon-1528972

Recientemente, para ser exactos, en junio de 2015, Corea del Norte, amenazó con llevar a la ruina a EE.UU. a través de una ciberguerra. Según TIC Beat (2015), el propósito de las autoridades coreanas es emprender una ciberguerra contra Estados Unidos y sus aliados, cuyo texto fue publicado en el *Rodong Sinmun,* periódico más popular del régimen coreano.

Por lo anterior, los ciberataques proceden también de actores tanto estatales como no estatales, no solo de *hackers*, además de terroristas, grupos extremistas, criminalidad organizada, etc. Consideran Arquilla y Ronfeldt (1997), que actores no estatales como Al–Qaeda o ciertos grupos antisistema, son modelos pragmáticos de organizaciones terroristas en red.

De tal forma que en el espectro del ciberespacio a través de las TIC se pueden desarrollar misiones de engaño electrónico, confundir sistemas de inteligencia, mando y control, comunicaciones y otros articulados con la red. Tanto así, que tal perturbación puede ser devastadora para el personal, equipo, instalaciones o cualquier tipo de infraestructura crítica.

Esta situación se torna crítica, pues en el mundo globalizado las sociedades son dependientes de los sistemas en red que dominan el ciberespacio. Para Gaitán (2011), tales actividades de dependencia de redes computarizadas y del ciberespacio, incrementan los niveles de vulnerabilidad de la Seguridad y Defensa Nacional. Según la QDR[9] (2010), solo el Pentágono sufre más de 5.000 ciberataques diarios. Por tal motivo, el concepto del campo de batalla dentro del teatro de la ciberguerra debe visualizar un punto focal en defensas cibernéticas y previsión de ataques sorpresivos, desarrollando estrategias de contención contra dicha amenaza global.

Para el Departamento de Defensa de EE.UU. el ciberespacio es un dominio global dentro del ambiente de información compuesta por

9 Estrategia d Defensa Cuadrienal de EE.UU. de febrero de 2010.

> la red interdependiente de infraestructuras de Tecnologías de la información donde la electrónica y el espectro electromagnético confluyen para almacenar, modificar o intercambiar datos a través de sistemas en red e infraestructuras físicas asociadas[10] (Schmitt, 2012, p. 245).

Por lo anterior, las Fuerzas Militares deben adaptarse al mundo globalizado en el cual, la sociedad opera en red, y en donde el concepto de guerra virtual librada en el ciberespacio, puede integrar plataformas, sistemas, sensores, y otros actores operando con rapidez, efectividad y precisión. Un ejemplo de ello, se presentó en la primera guerra del golfo, cuando la CÍA a través de un *chip* con virus puesto en dispositivos de comunicaciones e impresoras adquiridas por Irak, permitió neutralizar los dispositivos de defensa antiaérea, haciéndolos inservibles antes del bombardeo estratégico estadounidense (Rodríguez, 2012).

El nuevo campo de combate virtual[11] pone en entredicho las garantías existentes sobre el uso de tecnologías de la información y las comunicaciones en este espacio, que a pesar de lo ventajoso, es vulnerable frente a actores que buscan satisfacer sus necesidades más allá de lo ilegal. Por ello, por ejemplo, EE.UU, inició un proceso a cinco funcionarios chinos de la Unidad de Ciberdefensa 61398[12] en Shanghái, por encontrarlos responsables de ciberataques contra el Gobierno estadounidense en 2014, infectando redes informáticas de varias empresas gubernamentales en Washington (Sierra, 2015).

El nuevo campo de combate virtual para las Fuerzas Militares de Colombia.

La integración en red del mando en todos los niveles, permite al Comandante controlar virtualmente y en forma detallada el campo de batalla, manejar las comunicaciones, tanto horizontales como verticales, y coordinar el poder político y los mandos subalternos en el terreno. Por tanto, es necesario proteger ese espacio para que no sea vulnerado y los datos en el ciberespacio no sean alterados. Más aún, las Fuerzas Militares deben buscar acomodar el nuevo campo de combate virtual a su favor.

> "... en 2007 diversos sistemas de Estonia fueron afectados masivamente por un ataque de denegación de servicio como consecuencia de la decisión del gobierno de remover un monumento ruso que representaba para Rusia la liberación de Estonia, de Hitler".

En Colombia la mayor parte de la infraestructura crítica no está conectada con la red. Nuestros sistemas de gas, agua, trasporte, no se conectan aún a las redes de internet como en Estados Unidos. Según Andrés Velázquez (Pérez, 2012), ingeniero cibernético y director de **Mattica**, el primer laboratorio de investigación de delitos informáticos de América Latina, esto hace que el ciberterrorismo y la ciberguerra no sean una amenaza inminente. Sin embargo, de acuerdo con lo expuesto en párrafos anteriores, existen diversas áreas de vulnerabilidades a ciberataques y otros riesgos del ciberespacio.

En 2007, Colombia reportó pérdida de 6.6 billones de pesos a raíz de delitos informáticos, por ello, dada la vulnerabilidad del ciberespacio, en Colombia se puso en marcha la *Ley 1273 de 2009*, creando nuevos tipos penales relacionados con delitos informáticos[13] y la protección de la información y de los datos con penas de prisión de hasta 120 meses y multas de hasta 1.500 salarios mínimos legales mensuales vigentes.

10 Incluyendo internet, redes de comunicaciones, sistemas informáticos, procesadores y controladores.

11 Conocido como el quinto poder. La estrategia de acción incluye por primera vez al ciberespacio como área de operaciones paralela al espacio, tierra y mar.

12 Segunda Unidad de Ciberdefensa más grade del mundo, ubicada en Shanghái sobre la calle Datong.

13 La *Ley 1273* establece como delitos informáticos el robo de información, robo de recursos, retardo y obstaculización en procesos, así como la destrucción material.

Foto: William Malagon

Aunado a ello, a partir de julio de 2011 nacen los lineamientos de las políticas de ciberseguridad y ciberdefensa a través del documento Conpes 3107, cuyo objetivo es fortalecer las capacidades del Estado para prevenir o enfrentar riesgos en el ámbito cibernético, cuyo impacto amenaza la seguridad del Estado y donde el ciberdelito abarca una amplia diversidad de actividad criminal (Ambos, 2015, pág.11).

Por el anterior, el Conpes 3107 se convierte en el documento rector para nuevas organizaciones estructurales que buscan responder a las demandas de seguridad en el ciberespacio, a la protección del individuo, los activos críticos y la unificación de la estrategia, entre ellas COLCERT[14] y otras.[15] Sin embargo, la ciberdefensa en el Estado colombiano ha sido relevante, pero no ha cobrado un alto grado de importancia en los niveles operativo y táctico que coadyuven a la Seguridad Nacional, pues aunque el nivel estratégico ha buscado determinadas medidas coordinadas con el sector público y privado, que le permita responder a cualquier agresión como respuesta a un ciberataque, no hay claridad acerca de lo que se considera como agresión a la seguridad desde el ciberespacio en los mandos subordinados.

Lo anterior, deja en evidencia que hay un escaso conocimiento del concepto de ciberespacio en el interior de los miembros de las Fuerzas Armadas colombianas, que sumado a la evidente falta de normatividad y a la dependencia de la comunidad internacional, por estar a la merced de sus legislaciones, se constituye como un obstáculo que debe ser superado. Pues bien, "como consecuencia de esa posición de privilegio con que parten los gigantes de internet[16] puede que marchemos hacia un ciberespacio autorregulado." (Instituto Español de Estudios Estratégicos

14 Grupo de respuestas a emergencias cibernéticas de Colombia. Se recomienda ver: http://www.colcert.gov.co/?q=preguntas-frecuentes

15 CCOC (Comando Conjunto Cibernético), integrado en las Fuerzas Militares de Colombia.

16 Países industrializados, o grandes coaliciones que aventajan a los viejos estados-nación sobre el quinto dominio.

pág.113, p. 1). Hoy grandes y pequeños actores del ciberespacio libran una batalla por el control o descontrol del mismo. Los países tercermundistas tienden a posturas de dependencia frente a los intereses de otros Estados más fuertes. Para los viejos Estados-nación, que se debaten entre dificultades sociales y financieras, sus decisiones y legislación están sujetas a los dictados de actores estatales y no estatales con mayor poder. Sin embargo, en un contexto de guerra híbrida, los mismos actores pequeños pueden emprender acciones cibernéticas contra enemigos poderosos.

Así la estrategia global para el ciberespacio se centra en el objeto de cada organización:

> La Otan persigue la protección de los sistemas críticos para su misión, la Unión Europea la creación de un mercado digital único soportado por la internet segura y confiable; Naciones Unidas pretende hacer accesibles para todos, los beneficios de usos de las TIC y la internet. Incluso cuando un estado miembro pertenece a diferentes organizaciones, la representación de cada una de ellas frecuentemente recae sobre departamentos que no mantienen posturas ni concertadas ni coherentes. (Instituto español de estudios estratégicos, 2010, p.2010)

"... en el espectro del ciberespacio a través de las TIC se pueden desarrollar misiones de engaño electrónico, confundir sistemas de inteligencia, mando y control, comunicaciones y otros articulados con la red. Tanto así, que tal perturbación puede ser devastadora para el personal, equipo, instalaciones o cualquier tipo de infraestructura crítica".

Recomendaciones.

Lo anterior determina que estar bajo el actuar de la comunidad internacional no es lo más fac-

Foto: http://equilibrium-security.co.uk/whats-new-in-the-world-of-cyber-security/

"En 2007, Colombia reportó pérdida de 6.6 billones de pesos a raíz de delitos informáticos, por ello, dada la vulnerabilidad del ciberespacio, en Colombia se puso en marcha la Ley 1273 de 2009, creando nuevos tipos penales relacionados con delitos informáticos y la protección de la información y de los datos con penas de prisión de hasta 120 meses y multas de hasta 1.500 salarios mínimos legales mensuales vigentes".

tible, siendo necesario fortalecer los mecanismos internos, adelantando alianzas y procesos interagenciales a través de la cooperación entre socios y organizaciones que perciban la necesidad de la ciberseguridad en común acuerdo para castigar el crimen en el ciberespacio. Por ello, el Estado colombiano debe impulsar medidas de contención y prevención a través del Comando Conjunto Cibernético (CCOC), buscando una oportuna acción que permita el control del ciberespacio a través de ingeniería informática avanzada, así como otras herramientas, que permitan extender la red a la ventaja táctica.

Por ende, en el futuro, desde una perspectiva ofensiva y a través del nuevo campo de batalla virtual, las Fuerzas Militares deben lograr la capacidad de ejecutar operaciones [17] por medio de este dominio, sin interferencia prohibitiva en un momento dado. Ello con la dependencia de elementos de seguridad, reconocimiento y vigilancia, Inteligencia articulada de diferentes fuentes, conocimiento situacional y en tiempo real del campo de batalla, entre otros.

Al igual, el concepto defensivo[18] debe responder a acciones inminentes o en curso contra redes de las Fuerzas Armadas, negando la libertad de acción en el ciberespacio al enemigo. Es necesario defender para asegurar la integridad de la información interconectada al espacio de batalla. Se puede concluir que en el actual panorama donde las amenazas cibernéticas son cada vez mayores, el Estado colombiano debe aumentar la legislación y extender el conocimiento en temas de Seguridad y Defensa a través de la generación de doctrina para las Fuerzas Armadas. También debe mejorar las capacidades para responder o evitar ataques cibernéticos, más aún, a través de iniciativas orientar y fortalecer la infraestructura física e informática que permita contener la amenaza..

Pues bien, la ciberguerra no es una amenaza inminente para Colombia, sin embargo, pese a la vulnerabilidad de los ataques cibernéticos, las fuerzas del ciberespacio deberán adquirir capacidades ofensivas como defensivas, negando el uso del mismo a aquellos que pretendan atentar contra la Seguridad y Defensa del Estado. Estamos ante un nuevo escenario, parte de la evolución que se da

Referencias Bibliográficas.

» *Fuentes académicas*

➢ Arquilla, J & Ronfeldt, D. (1997). Athenea´s Camp: Preparándose para la guerra de la información, Santa Mónica.

➢ Ambos, K. (2015). Responsabilidad penal internacional en el ciberespacio. Fundación universitaria externado de Colombia editores.

➢ Cornell, E. & Star, F. (2009). The guns of august 2008. Guerra Rusa en Georgia. New york M.E. Sharpe. Pág. 123, 153

➢ QDR. (2010). Informe de Revisión de Defensa Cuadrienal de los USA. Estrategias de defensa.

17 Ataques de Red en Computadoras (CNA), Explotación de Red de Computadoras (CNE), pudiendo aplicar mecanismos de influencia. Todo esto permite tomar acciones decisivas contra los objetivos propuestos.

18 Obedece a la Defensa de la Red de Computadoras (CDN), puede contribuir con los mecanismos de influencia.

➢ Schmitt. (2012). Clasificación del ciberconflicto. Vol. 17. Pág. 245

➢ Sun tzu. (600 años a.c). El arte de la guerra.

» *Fuentes cibernéticas*

➢ Huerta P. Ciberguerras las batallas del futuro hoy. Recuperado el día 25 de julio del 2015 de http://id.tudiscovery.com/ciberguerras-las-batallas-del-futuro-hoy/Instituto español de estudios estratégicos. (Jun 1 de 2010). Retos y amenazas de la seguridad nacional en el ciberespacio. Editorial Ministerio de defensa. Vol. 149. Pág. 333.

➢ Instituto español de estudios estratégicos. (2010). Ciberseguridad retos y amenazas a la seguridad nacional en el ciberespacio. Edición 149. Ministerio de defensa editores. Recuperado el día 25 de julio del 2015 de http://www.defensa.gob.es/ceseden/Galerias/destacados/publicaciones/monografias/ficheros/126_EL_CIBERESPACIO_NUEVO_ESCENARIO_DE_CONFRONTACION.pdf

➢ Pérez, G. C(2012, Mayo 12). El enemigo está dentro de las organizaciones. El espectador. Recuperado el día 25 de julio del 2015 de http://www.elespectador.com/tecnologia/el-enemigo-esta-dentro-de-organizaciones-articulo-345652

➢ Rodríguez, D. (2012). El hegemonismo militar estadounidense. La revolución científico técnica actual aplicada al desarrollo del armamento. Nuevas concepciones para realizar la guerra imperial. Recuperado el 14 de mayo de 2015 de http://www.ceid.edu.ar/serie/2012/ceid_dt_105_rodrigo_d_rodriguez_angulo_el_hegemonismo_militar_estadounidense.pdf

➢ Sáenz, C. (2012). La ciberguerra en los conflictos modernos. Trabajo de investigación. Santiago. Recuperado el día 25 de julio del 2015 de http://www.academia.edu/9339213/LA_CIBERGUERRA_EN_LOS_CONFLICTOS_MODERNOS

➢ Sierra, G. (2015). Internet es el nuevo campo de batalla global. Clarin.com. Edición 25008. Recuperado el día 25 de julio del 2015 de http://www.clarin.com/mundo/Ciberguerra-Estados_Unidos-China-Gran_Bretana-NSA-Snowden-GCHQ_0_1333067115.html

➢ The Washington post. (06 jun. 2012). Stuxnet trabajado por EE.UU y expertos israelitas. Recuperado el día 25 de julio del 2015 de https://www.washintonngpos.com/world/national-security/stuxnet-was-wo-and-israeli-experts-officials-say/2012/06/01/gJQAInEy6U

➢ TIC Beat. (10 Jun de 2015). Corea del norte amenaza a estados Unidos con una ciberguerra. Universidad Piloto. Recuperado el día 25 de julio del 2015 de http://www.ticbeat.com/seguridad/corea-del-norte-amenaza-estados-unidos-con-una-ciberguerra/

➢ Wilson, Cl. (2008). CRS Reporte del congreso. Cibercrimen y ciberterrorismo. Recuperado el día 26 de julio de 2015 de http://www.fas.org/sgp/crs/terror/RL32114.pdf

CURRÍCULUM

Teniente Coronel Luis Martín Moreno: Miembro del equipo de investigación del Departamento Ejército de la Escuela Superior de Guerra, 2016. Magíster en Seguridad y Defensa Nacionales "Escuela Superior de Guerra" Fuerzas Militares de Colombia Bogotá. Especialista en Seguridad y Defensa Nacionales "Escuela Superior de Guerra" Fuerzas Militares de Colombia Bogotá. Especialista en Administración y Manejo de Recursos para la Seguridad Nacional.