Ciberseguridad y ciberdefensa: pilares fundamentales de la Seguridad y Defensa Nacional

Teniente Coronel Alexander Osorio Lalinde
Docente investigador ESDEGUE
* Coautoría con Giselle Lorduy López, Lina Amaya Henao y Tatiana Arenas Méndez.

Foto: Capital de Estonia.
Imagen recuperada de: fi compass
Link: https://www.fi-compass.eu/event/2292/financial-instruments-enhancing-sme-competitiveness-programming-period-2014-2020

Resumen

En las últimas dos décadas los Estados, organizaciones e individuos son altamente dependientes de la información concentrada en la web y de las herramientas tecnológicas. La conectividad brinda la oportunidad de obtener información en tiempo real, y a su vez, infiltrar, modificar, sustraer, manipular o infectar la información, en beneficio propio o de terceros.

Esto ha obligado a los Estados a que, a través de sus instituciones, formulen una estrategia adecuada, moderna y actualizada para enfrentar la ciberguerra, los ciberataques y el ciberterrorismo. El presente artículo abordará el tema de la Seguridad y Defensa nacional, desde la perspectiva tradicional de los conflictos surgidos entre dos Estados, y cómo estos emplean nuevos conceptos de guerra.

Actualmente la comunidad internacional atraviesa un momento coyuntural, derivado de varios fenómenos sociales y culturales que han modificado la visión de la guerra, pues esta se ha configurado, a lo largo de la historia, como la expresión más antigua que existe como medio de coerción hacia un grupo de individuos que por lo general no se identifican como iguales. Sin embargo, ¿es la guerra un fenómeno que solo se ejecuta para conseguir poder? ¿Qué es? ¿Se puede afirmar que existe un nuevo escenario global para su posible aplicación?

Para dar respuesta a los anteriores interrogantes se abordará en el artículo el cambio de las estrategias tradicionales, que en la actualidad se vienen aplicando en las guerras de cuarta y quinta generación. Las nuevas guerras presentan un sinnúmero de escenarios, que contrastan radicalmente con el concepto tradicional de la naturaleza de las guerras westfaliana y napoleónica, e incluso con aquellas que se dieron a principios del siglo XX. Las nuevas batallas han estado demandando de ejércitos cibernéticos y escenarios intangibles, como lo es el ciberespacio. El cibercrimen, los ciberataques e incluso el clímax del ciberterrorismo aún no han sido plenamente comprendidos.

1. DEFINICIÓN DE GUERRA, HIBRIDEZ Y CONFLICTOS ASIMÉTRICOS

La guerra puede entenderse como el rompimiento de la paz entre dos o más potencias, o la lucha armada entre dos o más naciones/bandos de una misma nación; en este caso, se entenderá que la guerra es un fenómeno que puede partir desde varias esferas: económica, política, social, religiosa, entre otras [1]. Sin embargo, la naturaleza de la guerra ha cambiado con el tiempo. En principio ofrecía aniquilar de manera total al enemigo, mientras que actualmente se puede argumentar que las guerras de cuarta y quinta generación producen tensiones más fuertes entre los actores involucrados, siendo los ciudadanos los más afectados (Derbent, 2006).

Según William Lind, la guerra de cuarta generación es el tipo de confrontación más peligroso que cualquier Estado ha tenido que enfrentar. Por ejemplo, la guerra contrainsurgente, la guerra contra el terrorismo, la guerra insurreccional, la guerra de desgaste, la guerra híbrida, la guerra sucia o desobediencia civil, entre otras. Denominadas las guerras del futuro, proponen la ampliación dimensional del campo de batalla, donde la sociedad es el centro de gravedad: el cambio de las acciones tácticas, que incluyen atacar el ámbito cultural enemigo, ofreciéndole a la población la opción de ser parte integral de la guerra, "el pueblo en armas" o "la hegemonía popular".

Las nuevas guerras vinculan otros actores que buscan demostrar o generar presión, imponiendo violencia a un Estado, gobierno u organización. Este nuevo escenario de guerras ha recurrido al desarrollo tecnológico, que pretende generar en el adversario un profundo daño, colapsando los sectores económicos, políticos, sociales y de seguridad. En este tipo de guerras no es necesario poseer infinidad de columnas de combatientes, porque lo más importante es contar con individuos que posean

1 Real Academia Española: es una institución cultural que se dedica a la regularización lingüística mediante la promulgación de normativas dirigidas a fomentar la unidad idiomática dentro y entre los diversos territorios.

una alta comprensión del entorno, del espectro y del contexto estratégico para llevar a cabo los ataques.

Las nuevas guerras requieren el establecimiento de acciones tácticas basadas en el uso de la tecnología y la información. La esencia del conflicto asimétrico y de convergencia criminal en los nuevos escenarios híbridos apunta a generar inestabilidad. El uso de los medios de comunicación masiva y las tecnologías de la información serán armas estratégicas y dominantes dentro de los nuevos escenarios de guerra.

El escenario principal de estas guerras es el manejo de las masas, tratando de conducir al individuo a que abandone su naturaleza social, para poder llevar las relaciones sociales a posibles hostilidades. Estos nuevos ataques hacen que se propaguen los conflictos asimétricos, entendiendo que: "Estas asimetrías, aunque no son en absoluto un fenómeno nuevo en el ámbito de la guerra, ya no constituyen una incidencia ocasional de determinadas batallas, sino que son una característica estructural de la guerra contemporánea" (Geiss, 2006, p. 1).

El gran desafío sobre este nuevo tipo de guerra reside en entender el poder, la precisión, la rapidez, la eficacia, la contundencia y la potencia con que los ataques traspasan y vulneran las fronteras geográficas de los Estados, a través de un concepto contemporáneo basado en la virtualidad. La hibridez y la asimetría en los conflictos actuales presentan, de *facto*, una nueva forma de abordar la guerra.

"Las nuevas guerras vinculan otros actores que buscan demostrar o generar presión, imponiendo violencia a un Estado, gobierno u organización. Este nuevo escenario de guerras ha recurrido al desarrollo tecnológico, que pretende generar en el adversario un profundo daño, colapsando los sectores económicos, políticos, sociales y de seguridad".

No se pretende, entonces, formular un nuevo paradigma que clasifique los nuevos ataques; sin embargo, se retoma el concepto de las guerras de quinta generación, el cual puede ser entendido como una nueva capacidad de los actores para alcanzar intereses nacionales, a través del uso de la fuerza cibernética e informática, y a su vez, el uso conceptual de la ciberguerra como elemento primordial para la obtención del poder. La ciberguerra ha tomado gran relevancia, debido a sus nefastos efectos, secuelas y consecuencias.

2. LOS NUEVOS FENÓMENOS

A lo largo de las dos últimas décadas se ha presentado un fuerte proceso de integración y automatización en la infraestructura de los diferentes Estados-Nación, no solo gracias al avance de las tecnologías de hardware y software, sino también mediante la expansión de la internet, la cual ha creado una dimensión espacial que combina lo virtual y lo real, denominada el ciberespacio (Higuera, 2013).

Ante el panorama que se presenta hoy en día, es posible ver un mundo cada vez más hiperconectado, pero susceptible a fenómenos de transformación social, económica y política. Así mismo, los Estados, de cara al nuevo milenio, son frágiles ante el sistema de factores de inestabilidad, que convergen con la criminalidad, el terrorismo y las insurgencias a través de la WEB, redes sociales, mensajería instantánea y mensajes encubiertos.

El ciberespacio se construye a través del intercambio de gran volumen de información, y convierte a este en una poderosa red que conecta ideas, individuos, actores no estatales, organizaciones y Estados, entre otros (Romero, 2004). Existe una realidad, que radica en que si bien el ciberespacio se ha utilizado para beneficio de la sociedad global, también es cierto que el fácil acceso a la red puede convertirse en una amenaza, no solo para los individuos, sino incluso para la seguridad de los Estados y la supervivencia humana.

> "Las redes sociales permiten que la información se extienda por el mundo a toda velocidad. Mientras que los beneficios son obvios y están documentados, este mundo hiperconectado podría permitir la rápida expansión viral de información engañosa o provocadora, con intención o sin ella, con consecuencias serias" (Bejarano, 2013, p. 2).

Por esta razón, el ciberespacio se ha trasformado en un campo de batalla que puede considerarse una amenaza para muchos Estados y actores; así, este nuevo escenario debería ser estudiado a fondo, tanto por los Estados como por las instituciones de seguridad y la academia. En la actualidad, las generaciones contemporáneas han adquirido la capacidad de comunicarse y compartir información de manera instantánea y a gran escala.

2.1. ESTUDIO DE CASO: ESTONIA, 2007

Un ejemplo de cómo un ciberataque puede resultar perjudicial para un país o una sociedad es lo ocurrido en Estonia, en el año 2007, donde una serie de ataques cibernéticos desestabilizaron al Estado, de modo que doblegaron y sometieron a las entidades públicas y privadas de ese país ante un adversario representado en una gran potencia mundial (Echeverry, 2016).

La infraestructura tecnológica y los servicios en línea de Estonia fueron irrumpidos, porque ese país no conocía el mapa sistémico de amenazas potenciales, ni comprendía el concepto de ciberseguridad y ciberdefensa. El ataque fue configurado a través de "infecciones locales, amenazas web, ataques en red, spam, e-mails infectados o escaneo bajo demanda" (Higuera, 2013).

El 12 de abril del 2007 se presentaron los hechos que desencadenaron los ataques; estos fueron causa de una decisión del gobierno estonio de retirar un monumento soviético llamado el "Soldado de Bronce de Tallin", el cual era una estatua que conmemoraba el sacrificio y valentía de los soldados soviéticos que murieron en combate durante la Segunda Guerra Mundial. Tal hecho condujo al malestar de la población

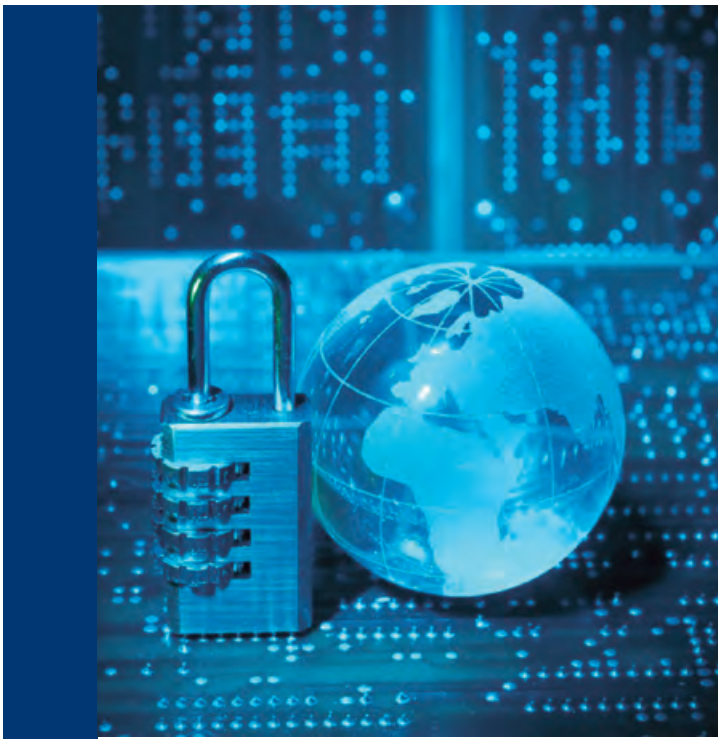
Foto: Evolución del ciberespacio en estonia.
Imagen recuperada de:Centre for International Governance Innovation
Link: https://www.cigionline.org/articles/doing-battle-cyberspace-how-attack-estonia-changed-rules-game

"A lo largo de las dos últimas décadas se ha presentado un fuerte proceso de integración y automatización en la infraestructura de los diferentes Estados-Nación, no solo gracias al avance de las tecnologías de hardware y software, sino también mediante la expansión de la internet, la cual ha creado una dimensión espacial que combina lo virtual y lo real, denominada el ciberespacio".

rusa presente en ese país, molestia consumada a través de manifestaciones y protesta social violenta a lo largo del territorio estonio.

Luego de estas manifestaciones se presentaron una serie de ataques a la plataforma digital, donde se evidenció una interrupción y denegación de los servicios públicos, que vulneraron la economía y los sistemas de información empleados por el Estado y las Fuerzas Militares de ese país. Estos ataques cibernéticos fueron lanzados por medio de sobrecargas, desconfiguración de las páginas web y avalanchas de correos no deseados recargados con virus, malware y spam, que afectaron toda la infraestructura electrónica, y paralizaron la economía y la infraestructura crítica nacional (Shakarian, Shakarian & Ruef, 2013).

Foto: Ciberseguridad
Recuperada de http://expansion.mx/opinion/2011/06/10/ipv6-mas-alla-del-limite-de-internet



Durante tres semanas, Estonia vio cómo su infraestructura crítica, de servicios tecnológicos y su red de internet pasaban de sufrir algunos tropiezos, a estar bajo la tutela y el control de una infiltración lógica externa, perdiendo así el monopolio de la economía y debilitando la estructura encargada de la defensa de los intereses del Estado. Fue tal la gravedad de los ataques, que se cerraron los sitios web de todos los ministerios, partidos políticos, algunos bancos y portales de medios de comunicación. Es importante señalar que la economía de este país se fundamenta principalmente en los servicios electrónicos y en las telecomunicaciones, aspecto por el cual los efectos devastadores de los ciberataques impactaron en forma considerable el producto interno bruto (PIB).

Según investigaciones de las autoridades de Estonia, que contaron con la colaboración de la Unión Europea y demás países miembros de la OTAN, se llegó a la conclusión de que los ataques cibernéticos habían sido realizados desde territorio ruso, en respuesta al traslado del monumento honorario a la Unión Soviética. Tal situación evidenció la fragilidad de las sociedades contemporáneas, como resultado directo de la hiperconectividad global y la fuerte dependencia de las tecnologías.

Esto ha obligado a los Estados a instrumentalizar las instituciones y tomar medidas que coadyuven a controlar el ciberespacio, tanto para el ataque como para la defensa, dada la naturaleza global de las actuales amenazas y de la preservación de los intereses nacionales. El procesamiento de la información, las redes de comunicación y la información han sido también el núcleo de cada actividad militar para lograr el dominio de todo el espectro (Visión Conjunta 2020, 2001).

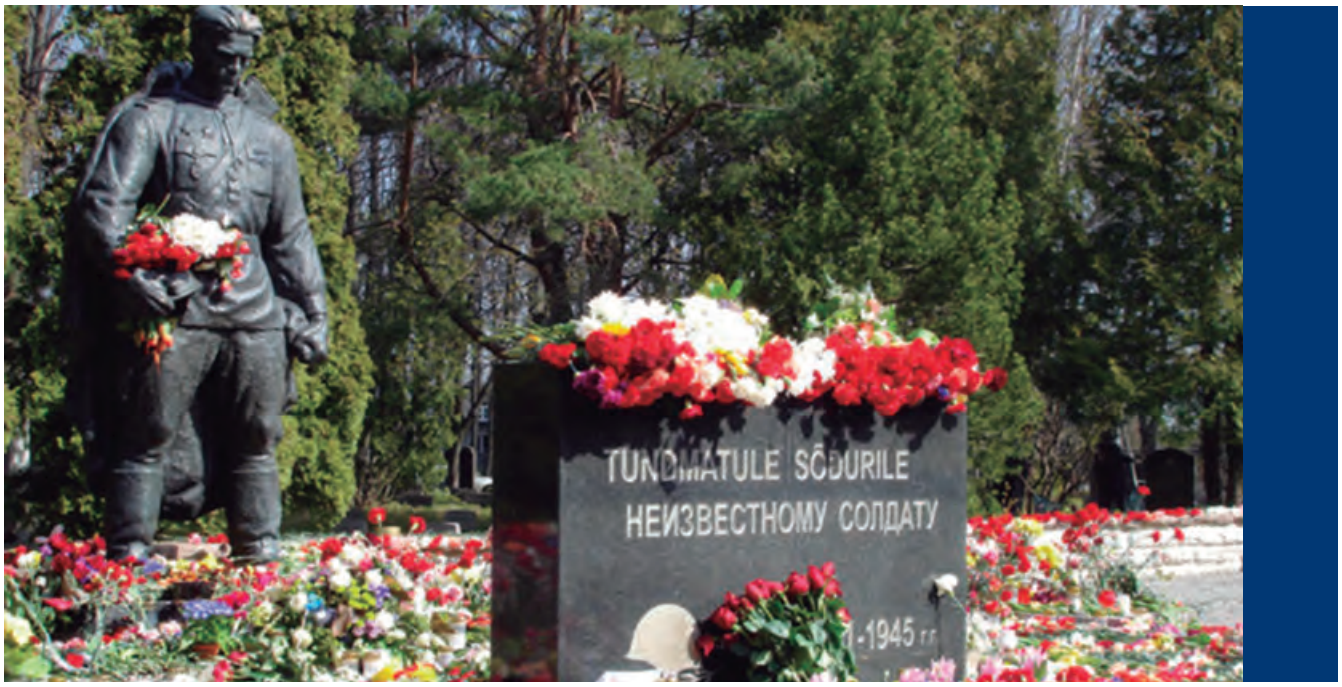


Foto: Soldado de Bronce en Tallin-Stonia
Imagen recuperada de: Information Portal to European Sites of Remembrance
Link: https://www.memorialmuseums.org/denkmaeler/view/1466/Bronzesoldat

3. CIBERSEGURIDAD Y CIBERDEFENSA

Del análisis anterior toman importancia los conceptos de ciberseguridad y ciberdefensa. La primera se refiere al conjunto de acciones pasivas y activas desarrolladas en el ámbito de las redes, sistemas, enlaces o equipos informáticos, a fin de salvaguardar estos para que cumplan su función, así como el empleo de políticas, conceptos de seguridad, directrices, métodos de gestión de riesgos, prácticas idóneas, seguros y tecnologías que pueden utilizarse buscando la integridad, autenticación, confidencialidad y no repudio, con el fin de proteger a los usuarios y los activos de la organización en el ciberespacio (CGFM, 2016).

Por otro lado, la ciberdefensa es el empleo de las capacidades militares ante las amenazas o actos hostiles de naturaleza cibernética, los cuales afectan a la sociedad, la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. De este modo, la tecnología, la ciencia y la innovación han sido fundamentales para la evolución humana; sin embargo, estos tres elementos, alineados con la ambición de poder, también representan una amenaza, a través del mal empleo de las tecnologías de la información, y se convierten en desafíos para la seguridad y estabilidad de los Estados (CGFM, 2016).

En Colombia, las primeras líneas de investigación sobre ciberseguridad y ciberdefensa se dieron

"Un ejemplo de cómo un ciberataque puede resultar perjudicial para un país o una sociedad es lo ocurrido en Estonia, en el año 2007, donde una serie de ataques cibernéticos desestabilizaron al Estado, de modo que doblegaron y sometieron a las entidades públicas y privadas de ese país ante un adversario representado en una gran potencia mundial".

"... la ciberdefensa es el empleo de las capacidades militares ante las amenazas o actos hostiles de naturaleza cibernética, los cuales afectan a la sociedad, la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales".

a partir del 2011, a través del documento CONPES 3701. Uno de los objetivos principales de este era la implementación de instancias apropiadas para prevenir, coordinar, atender, controlar, generar recomendaciones y regular los índices o emergencias cibernéticas, para afrontar posibles ataques o riesgos que atenten contra la seguridad nacional. En consecuencia, se crearon dos dependencias: la Comisión Intersectorial y el Grupo de Respuesta a Emergencias Cibernéticas de Colombia (COL CERT) (CGFM, 2016).

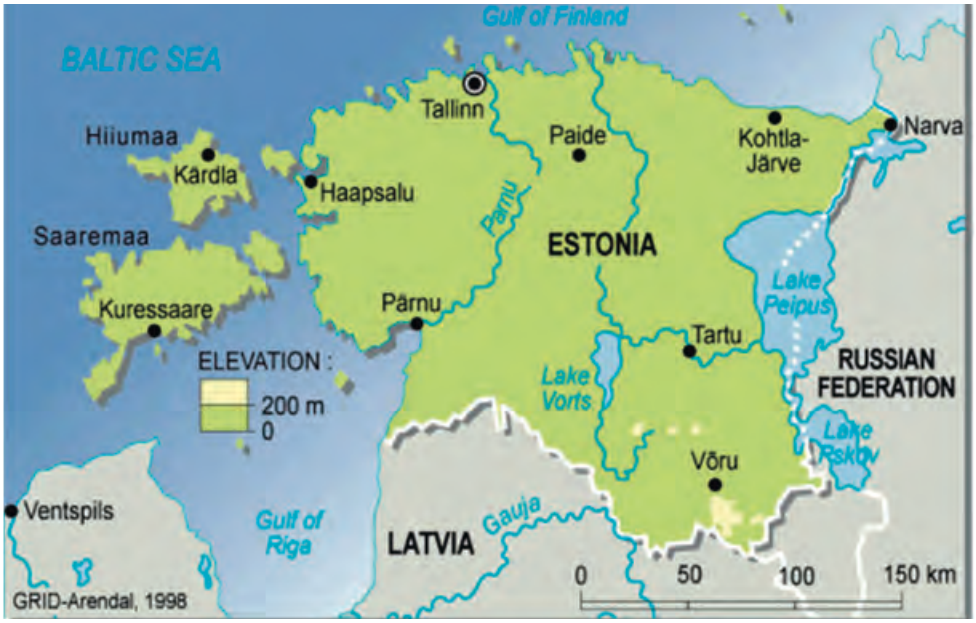
Entendiendo este importante reto para la seguridad nacional, la Escuela Superior de Guerra ha diseñado la Maestría en Ciberseguridad y Ciberdefensa, con el fin de profundizar en las temáticas más relevantes de la estrategia, normatividad y tecnología en el ciberespacio. De esta manera, se busca formar asesores e investigadores que sean capaces de prevenir la materialización de los riesgos cibernéticos en sus sectores de desempeño y garantizar la resiliencia en la operación de las infraestructuras nacionales. Este programa busca que cada egresado vele por la protección de las infraestructuras críticas del país, bajo un enfoque de riesgo operacional y resiliencia organizacional, apoyando el liderazgo regional y el progreso del país.

4. CONCLUSIONES

Los avances tecnológicos presentan realidades inimaginables para los seres humanos en las sociedades actuales; por esto, el ciberespacio se convierte en un activo estratégico, que requiere de toda la atención de los Estados para que pueda ser dominado y explotado en todas sus dimensiones, privando al adversario de controlar este, con el fin de no ser vulnerables ante un ciberataque.

Los Estados continúan observando grandes desafíos, al no adoptar contramedidas para evitar que los ataques cibernéticos, que son infligidos a través del poder, la precisión, la rapidez, la eficacia, la contundencia y la potencia, continúen ocasionando daños irreparables en la economía y estabilidad de las naciones.

Foto: Mapa de Estonia
Imagen recuperada de: https://ndie.pl/polska-zyskala-sojusznika-estonia-sprzeciwia-sie-karaniu-polski-odmowe-przyjecia-uchodzcow/



Internet, las redes sociales y la web actualmente se consolidan como los medios de comunicación más eficaces y poderosos del globo. Estos son preponderantes para establecer las relaciones entre los diversos actores que convergen en el sistema internacional; por esto, la ciberseguridad y la ciberdefensa se convierten tal vez en uno de los puntos más importantes para las agendas políticas de los actuales gobiernos.

El continuo uso de los medios de comunicación masiva y las tecnologías de la información se ha estado convirtiendo en un arma estratégica para dominar adversarios y doblegar voluntades. Es fundamental comprender que el sistema de factores de inestabilidad requiere de los escenarios híbridos para generar inseguridad.

Los actores criminales, terroristas, insurgentes, así como los Estados, compiten por el dominio del ciberespacio. De esta manera, es importante subrayar que las guerras de cuarta y quinta generación requieren cada vez más del uso de la web y de la información, porque el espectro de las operaciones militares deberá abarcar el control y dominio del ciberespacio.

Finalmente, en la era de la globalización, los Estados más poderosos continúan siendo vulnerables y frágiles ante las amenazas y ataques que se ciernen en el ciberespacio. A pesar de que países como los EE. UU., el Reino Unido y Francia destinan miles de millones de dólares en economía de defensa, desarrollo tecnológico e innovación, la población, la infraestructura crítica y la economía continuarán en riesgo.

"Internet, las redes sociales y la web actualmente se consolidan como los medios de comunicación más eficaces y poderosos del globo. Estos son preponderantes para establecer las relaciones entre los diversos actores que convergen en el sistema internacional; por esto, la ciberseguridad y la ciberdefensa se convierten tal vez en uno de los puntos más importantes para las agendas políticas de los actuales gobiernos".

El Estado colombiano enfrenta un reto importante en materia de seguridad y defensa; mientras no se controle correctamente el ciberespacio y se amplíen los conocimientos en esta dinámica, será difícil encontrar la estabilización en el sistema internacional. La academia y la ciencia bien direccionadas serán fundamentales para restringirle al adversario el empleo de la red y los medios de información a su favor.

Bibliografía

- BBC Mundo (2016, julio). Ataque en Niza: al menos 84 muertos al arrollar un camión a una multitud que celebraba la fiesta nacional de Francia. *BBC Mundo*. Recuperado de http://www.bbc.com/mundo/noticias-internacional-36800755

- Bejarano, M. (2013) *Algunos riesgos mundiales en un mundo hiperconectado.* Madrid: Instituto Español de Estudios Estratégicos.

- Castells, M. (2006). *La Sociedad en red: Una visión global*. Hellín, España: Alianza Editorial.

- CGFM (Comando General Fuerzas Militares de Colombia) (2016). CRE-i5. Ciberseguridad y ciberdefensa.

- Derbent, T. (2006). *Clausewitz, Mao y el maoísmo.* Recuperado de http://www.agota.be/t.derbent/articles/MaoClausESP.pdf

- Echeverry, L. M. (2016). *La relación de la ciberguerra con la guerra interestatal clásica: Estudio de caso Estonia, Georgia e Irán* (trabajo de pregrado). Universidad Militar Nueva Granada, Bogotá, D. C., Colombia.

- Enciclopedia de Ciencias Sociales - U. de Málaga. España - Clausewitz - Keegan.

- Geiss, R. (2006). Las estructuras de los conflictos asimétricos. *International Review of the Red Cross.* Recuperado de https://www.icrc.org/spa/assets/files/other/irrc_864_geiss.pdf

- Higuera, J. (2013). ¿Ciberguerra o ciberseguridad? *Tecnología Militar.*

- Kozlowski, M. (2014, febrero). Comparative analysis of cyberattacks on Estonia, Georgia and Kyrgyzstan. *European Scientific Journal*, 3, pp. 237-245. Recuperado de: http://www.eujournal.org/index.php/esj/article/viewFile/2941/2770

- Ministerio de las Tecnologías y la Información (2011). Lineamientos de Política para Ciberseguridad y Ciberdefensa. Recuperado de https://www.mintic.gov.co/portal/604/articles-3510_documento.pdf

- Reinares, F. (2015). Real instituto Elcano Royal Institute. Yihadismo global y amenaza terrorista: de al-Qaeda al Estado Islámico. Recuperado de http://www.realinstitutoelcano.org/wps/portal/rielcano_es/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_es/zonas_es/ari33-2015-reinares-yihadismo-global-y-amenaza-terrorista-de-al-qaeda-al-estado-islamico

- Revilla, M. & Hovanyi, R. (2013). La *"primavera árabe" y las revoluciones en Oriente Medio y Norte de África: episodios, acontecimientos y dinámicas.*

- Romero, J. (2004). *Ciberespacio y comunicación: nuevas formas de vertebración social en el siglo XXI.* Revista de estudios literarios de la Universidad Complutense de Madrid. Recuperado de http://www.biblioteca.org.ar/libros/150717.pdf

- Shakarian, P., Shakarian, J. & Ruef, A. (2013). *Introduction to Cyber-Warfare: A multidisciplinary approach.* Massachusetts, Estados Unidos: Elsevier.

- Soengas, X. (2013). El papel de Internet y de las redes sociales en las revueltas árabes: una alternativa a la censura de la prensa oficial. *Comunicar*, vol. XXI, N.º 41.

- Visión Conjunta 2020 (2001, diciembre). Las *Fuerzas Armadas de los EE. UU. preparándose para el futuro* (pp. 4-21). Join Force Quarterly.

CURRÍCULUM

Teniente Coronel Alexander Osorio Lalinde: Oficial del Ejército Nacional, del arma de Caballería en el grado de Teniente Coronel. Magíster en Estudios Internacionales de la Universidad de Wollongong, NSW, Australia. Su pregrado fue desarrollado en Ciencias Militares, con énfasis en Docencia para la Educación Superior y Universitaria en la Escuela Militar de Cadetes "General José María Córdova". Ha adelantado diplomados en Historia Militar, Derechos Humanos, Derecho Internacional de los Conflictos Armados, Contratación Estatal, temáticas fundamentales para el Ejército Nacional: Ley 1448 de 2011, y Planeación Estratégica. Adicionalmente, cuenta con especializaciones en Administración de Recursos Militares para la Defensa Nacional, Seguridad y Defensa, Liderazgo y Toma de Decisiones. Además, adelantó cursos en mantenimiento de paz y resolución de conflictos internacionales, implementación de las resoluciones del Consejo de Seguridad de la ONU sobre la agenda de la mujer, la paz y la seguridad en América Latina y el Caribe, así como en conducción de operaciones de ayuda humanitaria con la ONU. Actualmente se desempeña como Jefe del Departamento de Relaciones Civiles y Militares de la Escuela Superior de Guerra "General Rafael Reyes Prieto".

Lina María Amaya Henao: Estudiante de último semestre de Relaciones Internacionales y Estudios políticos de la Universidad Militar Nueva Granada.

Gisell Lorduy López: Estudiante de último semestre de la universidad Colegio Mayor de Nuestra Señora del Rosario en el pregrado de Relaciones internacionales.

Tatiana Arenas Méndez: Estudiante de último semestre de Negocios y Relaciones Internacionales de la Universidad de la Salle.