Ciberespacio:

nueva fuente de amenazas contra la seguridad nacional

Mayor Andrés Fernando Niño Wilches
Oficial de la Fuerza Aérea Colombiana
Alumno del Curso de Estado Mayor "CEM" 2014 - ESDEGUE

Carácter de las amenazas

Durante este siglo, las organizaciones internacionales como la Organización de las Naciones Unidas (ONU), la Organización de Estados Americanos (OEA) y sus Estados miembros, comenzaron a preocuparse por los nuevos desafíos y amenazas que atentan contra la estabilidad y la seguridad mundial.

"A principios del año 2002, en el marco de la Asamblea General de las Naciones Unidas, en la Resolución No 57-53, los Estados miembros manifestaron su preocupación por la utilización de medios y tecnologías de información en contra de la estabilidad y seguridad internacional; ya que la infraestructura de los Estados se afecta negativamente y, por ende, la seguridad civil y militar".

Por un lado, la OEA, mediante la Declaración de Bridgetown, es específica y categórica en determinar que estos desafíos "son de naturaleza diversa y tienen un alcance multidimensional"; por tal motivo, es importante trabajar en la identificación, clasificación y definición de los mismos.

Por otro lado, la Junta Interamericana de Defensa (2014),cuya función principal es la de prestar a la OEA y a sus Estados miembros los servicios de asesoramiento técnico, consultivo y educativo sobre temas relacionados con asuntos militares y de defensa en el hemisferio, presentó, en el mes de septiembre de 2001, un informe titulado *"Hacia un nuevo sistema de seguridad Hemisférica"*, en el cual se establecían las nuevas amenazas y las clasificaba en tres grandes categorías que en adelante se describen.

Las amenazas tradicionales: son las que involucran actores estatales, atentan contra la defensa del Estado, buscan afectar los campos del poder (político, económico, social y militar) y, para enfrentarlas, se requiere del empleo de la Fuerzas Militares.

Las amenazas no tradicionales: son las que involucran tanto actores estatales, como no estatales; son de carácter asimétrico; no requieren obligatoriamente de una acción militar; sin embargo, exponen al Estado y a sus instituciones.

Las amenazas estructurales: son las de carácter multidisciplinario, la necesidad de intervención militar es casi nula; por el contrario, requieren de una acción integral en el campo político, económico, social y tecnológico.

Por lo anterior, la clasificación de las amenazas se relaciona en el Cuadro 1.

Cuadro 1
Clasificación de las amenazas

Amenazas tradicionales	Amenazas no tradicionales	Amenazas estructurales
Armas de destrucción masiva	Terrorismo	Pobreza
Problemas limítrofes pendientes	Tráfico de drogas ilícitas y narcoterrorismo	Degradación del medio ambiente
Lucha por recursos vitales	Crimen organizado internacional	Corrupción
Lucha antiguerrillera e insurgencia	Problemas tribales, étnicos, políticos internos	Migración masiva y descontrolada
	Catástrofes Naturales	Violencia ciudadana
	Transporte y depósitos de desechos nucleares radioactivos	VIH/SIDA y enfermedades epidémicas
	Tráfico ilícito de armas	Diferencia tecnológica
	Crimen cibernético	Desempleo
	Lavado de dinero	Crisis económica
	Tráfico de personas	

Fuente: Junta Interamericana de Defensa

Alcance de las Ventajas Vs. las desventajas

Así mismo, a principios del año 2002, en el marco de la Asamblea General de las Naciones Unidas,

Foto: www.worriors

en la Resolución No. 57-53, los Estados miembros manifestaron su preocupación por la utilización de medios y tecnologías de información en contra de la estabilidad y seguridad internacional; ya que la infraestructura de los Estados se afecta negativamente y, por ende, la Seguridad Civil y Militar. A su vez, se invitó a los Estados miembros a determinar los criterios básicos en cuanto a seguridad de la información, especialmente con el uso apropiado e ilícito de las tecnologías de la información y las telecomunicaciones (ONU, 2002b: pp. 1-3).

Posteriormente, la OEA, a través del Comité Interamericano Contra el Terrorismo (CICTE), en el marco del cuarto período de sesiones, celebrado en la ciudad de Montevideo, Uruguay, del 29 al 30 de enero de 2004, estableció el compromiso, por parte de los Estados miembros, para identificar y combatir las amenazas emergentes, tales como las amenazas a la seguridad cibernética (OEA, 2004).

Estas amenazas surgen del continuo desarrollo tecnológico en materia de comunicaciones, sistemas y tecnologías de la información, las cuales dieron origen al dominio creado por el hombre, "el ciberespacio"; este, como tal, ha generado un sinnúmero de ventajas.

En el campo económico, Internet y las TIC han transformado nuestra sociedad; permiten que miles de organizaciones sean más eficientes, maximicen el uso de sus activos, incrementen los niveles de producción, realicen la comercialización a un menor costo y desarrollen modelos innovadores de negocio; adicionalmente, crearon las bases para la globalización y la internacionalización de muchas compañías, lo que favorece el crecimiento económico de muchos países.

El ciberespacio ha creado una nueva forma de hacer negocios, el comercio electrónico ha crecido ostensiblemente. Según cifras de la Cámara Colombiana de Comercio Electrónico (CCCE), durante 2013, se registraron ventas alrededor de los 2.500 millones de dólares; ello equivale a un aumento del 40%, con referencia al año 2012 (Portafolio, 2014), lo que representa el 0,12% del PIB (DNP, 2009).

A nivel social, la interconectividad a través de las redes de información ha facilitado el acceso al

conocimiento, a la información y a la educación, permitiéndoles realizar proyectos colaborativos para llegar a diferentes mercados alrededor del mundo. Asimismo, ha permitido la conexión de millones de personas al ofrecer nuevas formas de comunicación y cooperación entre sí (chats, redes sociales, comunicaciones basadas en IP,...).

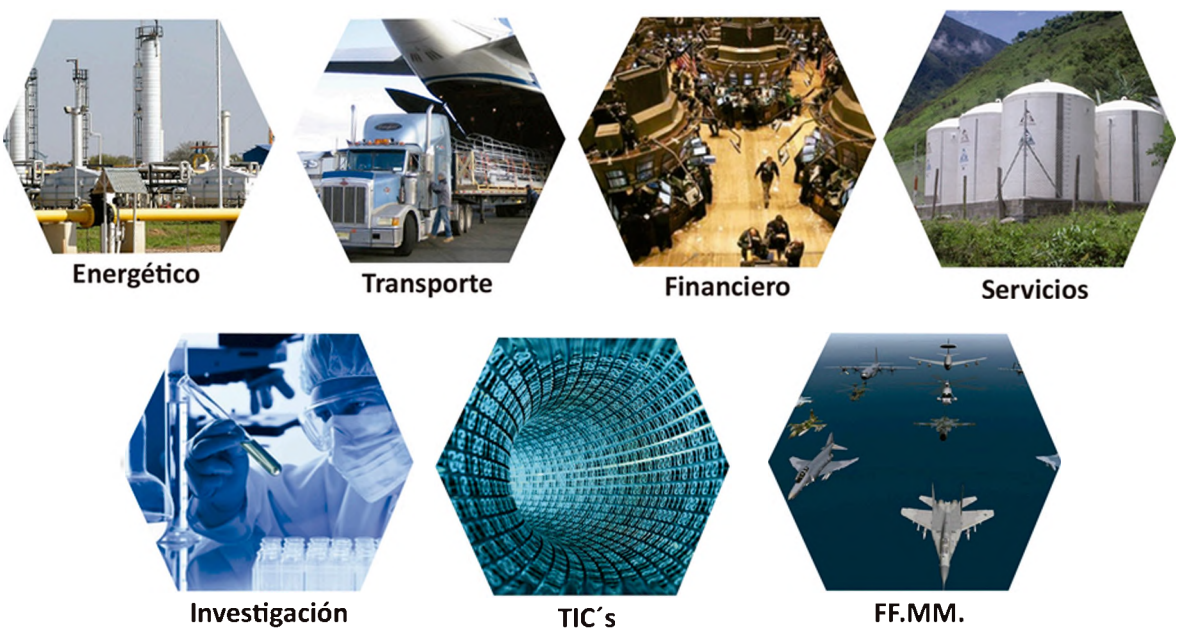
Internet se hizo pública a partir del año 1991 y, actualmente, existen alrededor de 2.4 billones de personas usuarias, casi un tercio de la población mundial; en el caso de Colombia, los usuarios de internet ascienden a 26.936.343 millones de personas, lo que equivale al 59.9% de la población.

En el campo militar, también se han obtenido ventajas significativas. Desde que se introdujeron los computadores y la transmisión de datos por internet en la Guerra del Golfo Pérsico en el año 1991, las Fuerzas Militares, en sus centros de operaciones, contaron con información en tiempo real acerca de la ubicación de sus Unidades y la situación en el campo de batalla; lo cual le facilitaba a los comandantes el proceso de toma de decisiones. Esto, sumado a la capacidad de realizar la entrega de armamento de una forma más precisa, reduce, de manera significativa, los daños colaterales durante el desarrollo de las operaciones militares.

Como se puede observar, el ciberespacio ha traído grandes ventajas a los Estados y al desarrollo de cada uno de los campos del poder; mas, no todo es positivo, dado que se ha generado una alta dependencia a las TIC, hasta el punto de convertirse en indispensables para el funcionamiento de los países, sus infraestructuras críticas y sus Fuerzas Armadas. La Figura 1 así lo ilustra.

Figura 1

Principales sectores de Infraestructura crítica



Fuente: elaboración propia basada en documentación examinada

Las proyecciones

La dinámica del desarrollo tecnológico muestra que la dependencia seguirá aumentando en el futuro. Las redes y los sistemas de la información hacen posible muchos de los procesos de los sectores energético, financiero, transporte, servicios, salud, y, a las Fuerzas Armadas, los procesos de operaciones, apoyo logístico, Inteligencia, entre otros; por tal motivo, las infraestructuras tecnológicas que hacen posible el flujo de estos datos se convierten en infraestructuras vitales para los Estados.

Es importante establecer la distinción entre los conceptos de infraestructuras tecnológicas y las infraestructuras críticas. Estas últimas corresponden a los sistemas físicos o virtuales que son vitales para el normal funcionamiento de los Estados, y que, de llegar a ser inhabilitados o destruidos, impactarían la estabilidad económica, la salud pública y, finalmente, el bienestar de la población. En conclusión, amenazan la Seguridad Nacional.

La interconectividad requerida para el funcionamiento de los diferentes sistemas que permiten el normal desarrollo de la sociedad moderna hace que estos sean altamente vulnerables ante ataques cibernéticos, los cuales se ven representados por algunos Estados Nación, actores trasnacionales, organizaciones cibercriminales, pequeños grupos o actores individuales, que buscan explotar las vulnerabilidades propias de la infraestructura de TI y de su interacción a través del ciberespacio.

Cuadro 2

Amenazas a la Seguridad Nacional

Amenaza	Metodología	Intenciones
Hackers	Ingreso a sistemas y redes privadas, vulnerando los sistemas	Robo, fraude, denegación de servicio y extorsión
Crimen Organizado	Aprovechar actividades online, descifrar códigos	Interés económico
Terroristas	Atacar sistemas conectados a la red	Adquirir información para el planeamiento de ataques físicos o cibernéticos
Estados Nación	Desarrollo de ciber-capacidades ofensivas, técnicas y operativas	Espionaje y ciberataques en el marco de una ciberguerra

Fuente: Office of the Homeland Security, National Strategy for Homeland Security

Ciberataques

Cuando se habla de ataques cibernéticos, se debe saber que son todas aquellas acciones deliberadas, cuyo fin es alterar, interrumpir, engañar, degradar o destruirlos sistemas informáticos, las redes, la información y/o los programas que residen o transiten dentro de estos sistemas (National Academic Press, 2009).

Existen antecedentes que permiten establecer que los ciberataques no son cosas del futuro, por el contrario, se han presentado ya hace casi una década, los cuales atacaban infraestructuras críticas de diferentes países y que afectan los diferentes campos del poder de un Estado.

Campo Político

En el mes de abril de 2007, el Gobierno de Estonia vivió una serie de ataques, en donde se vieron afectados la presidencia, el parlamento, la mayoría de los ministerios, los partidos políticos y dos de sus grandes bancos. Se presentó una importante interrupción de los servicios, con lo cual se buscaba ejercer presión política sobre el Gobierno georgiano y parecía estar coordinado con las acciones militares rusas. Este ataque desató una gran crisis que requirió la intervención de la comunidad internacional y alertó a la Organización del Tratado del Atlántico Norte, Otan (Nato Review Magazine, 2013).

Hackers atacaron la infraestructura de Internet de Israel durante la ofensiva militar de enero de 2009 en la Franja de Gaza. El ataque, que se centró en los sitios web del gobierno, fue ejecutado en, por lo menos, 5.000.000 de computadoras. Las ofensivas israelíes fueron realizadas por una organización criminal financiada por los grupos del Hamas o Hezbollah.

Campo Económico

El Gobierno canadiense informó, en el mes de enero de 2011, acerca de un ataque cibernético en contra de sus agencias, entre ellas, investigación y

"En el campo económico, Internet y las TIC han transformado nuestra sociedad; permiten que miles de organizaciones sean más eficientes, maximicen el uso de sus activos, incrementen los niveles de producción, realicen la comercialización a un menor costo y desarrollen modelos innovadores de negocio; adicionalmente, crearon las bases para la globalización y la internacionalización de muchas compañías, lo que favorece el crecimiento económico de muchos países".

desarrollo para la defensa de canadá, el departamento de Finanzas y del Consejo del Tesoro, principales organismos económicos de Canadá, los cuales se vieron obligados a desconectarse de Internet.

En el mes de julio de 2013 la compañía Symantec informó acerca de una significativa cantidad de ataques dirigidos hacia las empresas de generación y distribución de electricidad, operadoras de oleoductos, proveedores de equipos industriales para el sector energético e hidrocarburos. La mayoría de las empresas afectadas fueron en los EE.UU., España y Francia; pero, también incluyó a empresas de Italia, Alemania, Turquía, Polonia, Rumania, Grecia y Serbia (Symantec, 2014).

Campo Militar

En el mes de Octubre de 2012, la firma Kaspersky descubrió un ataque cibernético a nivel mundial llamado "Octubre Rojo", ejecutado desde el año 2007. Los países que fueron objeto de este ataque, fueron países de Europa, la antigua Unión Soviética, Asia Central, y América del Norte.

Los hackers obtuvieron información altamente confidencial de embajadas del gobierno, empresas de investigación, instalaciones militares, proveedores de energía, plantas de energía nuclear y otras infraestructuras críticas.

Colombia enfrenta las nuevas amenazas

Como se puede evidenciar, existe una amenaza latente contra las infraestructuras que permiten el normal funcionamiento de cada uno de los sectores del país y el bienestar de la población, por tal motivo el Gobierno colombiano inició, desde el año 2011, una estrategia de ciberseguridad y ciberdefensa que permita protección de los altos intereses nacionales de todas aquellas amenazas internas y externas provenientes del ciberespacio que puedan constituirse, en determinado momento, en obstáculos.

Hoy el país cuenta con entidades que se encargan de enfrentar las amenazas provenientes del ciberespacio, entre ellas están:

- El Grupo de Respuesta a Emergencias Cibernéticas de Colombia (colCERT), cuya responsabilidad es la coordinación de la Ciberseguridad y Ciberdefensa Nacional. La coordinación de las acciones necesarias para la protección de la infraestructura crítica del Estado colombiano frente a emergencias de ciberseguridad que atenten o comprometan la Seguridad y Defensa Nacional (Disponible en http://www.colcert.gov.co/?q=acerca-de.).
- El Comando Conjunto Cibernético, organización del Comando General de las Fuerzas Militares de Colombia, cuya misión es prevenir y contrarrestar toda amenaza o ataque de naturaleza cibernética que afecte los valores e intereses nacionales (DNP,

2011). Asimismo, el Ejército Nacional, la Armada Nacional y la Fuerza Aérea crearon sus Unidades de Ciberdefensa, las cuales les permiten proteger sus infraestructuras ante las nuevas amenazas y, así, garantizar el cumplimiento de la misión asignada a cada una de las Fuerzas.

- El Centro Cibernético Policial es la dependencia de la Dirección de Investigación Criminal e Interpol, encargada del desarrollo de estrategias, programas, proyectos y demás actividades requeridas en materia de investigación criminal contra los delitos que afectan la información y los datos (Disponible en Centro Cibernético Policial. http://www.ccp.gov.co/mision.php.).
- Igualmente, el Ministerio de Defensa Nacional, a través de la Escuela Superior de Guerra, inauguró, en el mes de mayo de 2013, el Centro Regional de Estudios Estratégicos en Seguridad (CREES), una institución que promueve el pensamiento estratégico en materia de seguridad y defensa, el trabajo conjunto para analizar y prevenir las nuevas amenazas a la seguridad nacional de los diferentes países del continente y estableció entre sus líneas temáticas la ciberseguridad y la ciber-

"... el ciberespacio ha traído grandes ventajas a los Estados y al desarrollo de cada uno de los campos del poder; mas, no todo es positivo, dado que se ha generado una alta dependencia a las TIC, hasta el punto de convertirse en indispensables para el funcionamiento de los países, sus infraestructuras críticas y sus Fuerzas Armadas".

Foto: Oficina de Prensa MinTIC

"Existen antecedentes que permiten establecer que los ciberataques no son cosas del futuro, por el contrario, se han presentado ya hace casi una década, los cuales atacaban infraestructuras críticas de diferentes países y que afectan los diferentes campos del poder de un Estado".

defensa, con el fin de analizar estos fenómenos y, de esta manera, diseñar las estrategias de mitigación y prevención (Disponible en Centro Regional de Estudios Estratégicos en Ciberseguridad. http://www.esdegue.edu.co/node/4465).

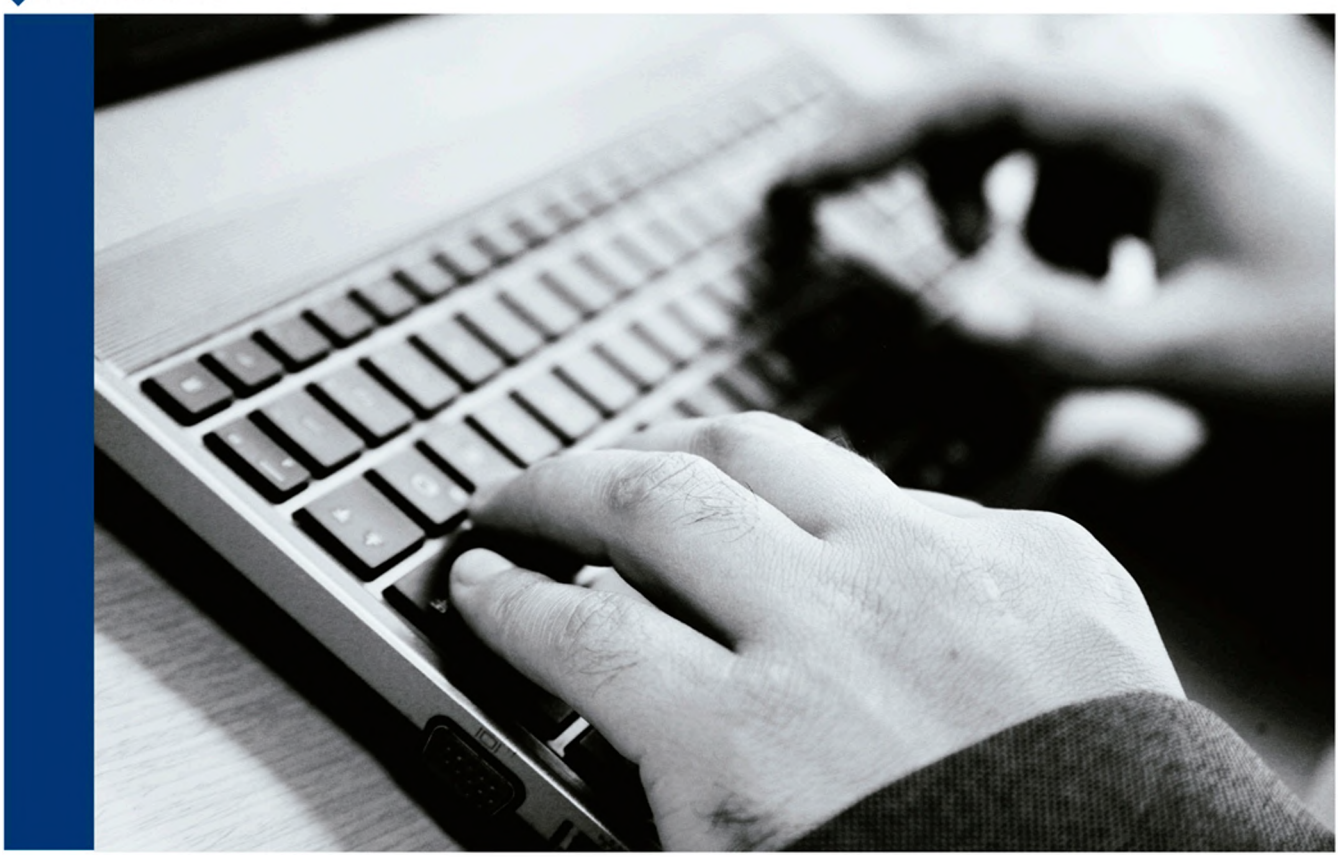
- Durante el año 2014, la Presidencia de la República ha estado trabajando en la propuesta de creación de la Agencia Nacional de Seguridad Cibernética, así como en la redacción de decretos para poner en marcha la Política Nacional de Ciberseguridad (Disponible en http://www.eltiempo.com/tecnosfera/novedades-tecnologia/colombia-se-prepara-para-enfrentar-los-ciberataques/14233838).

Conclusiones

A medida que pasa el tiempo y se desarrolla la tecnología, el ciberespacio nos ofrecerá nuevas y mejores oportunidades; será indispensable para nuestra sociedad, nuestra economía y el bienestar de los ciudadanos; sin embargo, a su vez, nos presentará nuevos retos frente a las crecientes y evolutivas amenazas, de manera tal que se debe estudiar, analizar y desarrollar capacidades para enfrentarlas y contrarrestarlas.

Aprovechar los acuerdos de cooperación entre los Estados miembros de las ONU y la OEA para fortalecer los procedimientos de intercambio de

Foto: Oficina de Prensa MinTic



"... el Ejército Nacional, la Armada Nacional y la Fuerza Aérea crearon sus Unidades de Ciberdefensa, las cuales les permiten proteger sus infraestructuras ante las nuevas amenazas y, así, garantizar el cumplimiento de la misión asignada a cada una de las Fuerzas".

información y de judicialización de las personas u organizaciones que atenten contra las infraestructuras de los Estados a través del ciberespacio.

Las instituciones creadas por el Gobierno Nacional son las llamadas a liderar los procesos de identificación de vulnerabilidades y aseguramiento de las infraestructuras críticas del país, en coordinación con los organismos públicos y el sector privado.

El país necesita un grupo significativo de profesionales capacitados y entrenados en materia de ciberseguridad, esto sumado al avance de proyectos de investigación y desarrollo permitirá que el país cuente con soluciones innovadoras para enfrentar dichas amenazas.

Se deben fortalecer las normas y los marcos jurídicos con el propósito de judicializar las personas que atenten contra la privacidad de las personas y contra las infraestructuras críticas, especialmente, las que permiten el normal funcionamiento de los diferentes sectores de la economía del país.

Bibliografía

Fuentes electrónicas

- CENTRO CIBERNÉTICO POLICIAL. http://www.ccp.gov.co/mision.php.
- CENTRO REGIONAL DE ESTUDIOS ESTRATÉGICOS EN CIBERSEGURIDAD. http://www.esdegue.edu.co/node/4465.
- COLCERT. http://www.colcert.gov.co/?q=acerca-de.
- COLOMBIA, DEPARTAMENTO NACIONAL DE PLANEACIÓN. Documento CONPES 3701. Lineamientos de política para ciberseguridad y ciberdefensa. Actualizado el 14 de julio de 2011. Citado el 12 de julio de 2014. Disponible en: http://www.mintic.gov.co/portal/604/articles-3510_documento.pdf.
- COLOMBIA, DEPARTAMENTO NACIONAL DE PLANEACIÓN. Piedrahita Uribe, Esteban. El comercio electrónico: una oportunidad para el desarrollo. Foro Nacional de Comercio Electrónico. Actualizado el 18 de junio de 2009. Citado el 12 de julio de 2014. Disponible en:https://www.dnp.gov.co/Portals/0/archivos/documentos/GCRP/Presentaciones_Escobar/Presentación_EP_Foro_Comercio_Electrónico.pdf.
- COMMITTEE ON OFFENSIVE INFORMATION WARFARE, NATIONAL RESEARCH COUNCIL. Technology, policy, law and ethics regarding U.S. acquisition and use of cyberattack capabilities. Ed. Owens, William A.; Dam, Kenneth W. y Lin, Herbert S. Washington: National Academic Press, 2009.
- EL TIEMPO.COM. Bogotá D.C. Colombia se prepara para enfrentar los ciberataques. sec. Tecnósfera. Actualizado el 14 de julio de 2014. Citado el 12 de julio de 2014. Disponible en: http://www.eltiempo.com/tecnosfera/novedades-tecnologia/colombia-se-prepara-para-enfrentar-los-ciberataques/14233838.
- INTERNET WORLD STATS. Estadísticas de uso y población. Actualizado el 25 de abril de 2014. Citado el 12 de julio de

2014. Disponible en: http://www.internetworldstats.com/stats3.htm.

- JUNTA INTERAMERICANA DE DEFENSA. Hacia un nuevo sistema de seguridad hemisférica. Actualizado el 22 de noviembre de 2010. Citado el 11 de julio de 2014. Disponible en: FAVOR INCLUIR EL LINK

- NATO REVIEW MAGAZINE. The history of cyber attacks – a timeline. Citado el 12 de julio de 2014. Disponible en: http://www.nato.int/docu/review/2013/Cyber/timeline/EN/index.htm.

- ORGANIZACIÓN DE LAS NACIONES UNIDAS. Resolución No. 57-53. 2002b, p. 1-3.

- ORGANIZACIÓN DE LOS ESTADOS AMERICANOS. AG/RES. 2004 (XXXIV-O/04). Reunión de Ministros de Justicia o de Ministros o Procuradores Generales de las Américas. Actualizado el 08 de junio de 2004. Citado el 11 de julio de 2014. Disponible en: http://www.oas.org/juridico/spanish/ag04/agres_2040.htm

- PORTAFOLIO.CO. Comercio electrónico, una tendencia en crecimiento. Actualizado el 03 de abril de 2014. Citado el 12 de julio de 2014. Disponible en: http://www.portafolio.co/economia/crecimiento-comercio-electronico-colombia

- SYMANTEC. Dragonfly: western energy companies under sabotage threat. Actualizado el 30 de junio de 2014. Citado el 12 de julio de 2014. Disponible en: http://www.symantec.com/connect/blogs/dragonfly-western-energy-companies-under-sabotage-threat

- WIKIPEDIA. Países por número de usuarios de Internet. Actualizado el 08 de abril de 2014. Citado el 12 de julio de 2014. Disponible en: http://es.wikipedia.org/wiki/Anexo:Pa%C3%ADses_por_número_de_usuarios_de_Internet.

CURRICULUM

Mayor Andrés Fernando Niño Wilches: Oficial de la Fuerza Aérea Colombiana, Administrador Aeronáutico (Escuela Militar de Aviación), Especialista en Alta Gerencia (Universidad Militar Nueva Granada), Especialista en Seguridad de la Información (Universidad de los Andes), candidato a magister en Gestión de Organizaciones (Universidad Militar Nueva Granada). Actualmente se encuentra adelantando Curso de Estado Mayor y la Maestría en Seguridad y Defensa Nacional en la Escuela Superior de Guerra.