AMENAZAS A LA INFRAESTRUCTURA DEL SECTOR DE TELECOMUNICACIONES (TIC) EN COLOMBIA

LADY CAROLINA LOZANO QUINTERO

UNIVERSIDAD MILITAR NUEVA GRANADA
FACULTAD DE RELACIONES INTERNACIONALES ESTRATEGIA Y SEGURIDAD
PROGRAMA DE RELACIONES INTERNACIONALES Y ESTUDIOS POLÍTICOS
BOGOTÁ D.C.

2015

AMENAZAS A LA INFRAESTRUCTURA DEL SECTOR DE TELECOMUNICACIONES (TIC) EN COLOMBIA

LADY CAROLINA LOZANO QUINTERO
0901386

Ensayo para optar al Título de
Internacionalista y politóloga

Tutor
Verena Lovich Villamizar
Administradora Pública

UNIVERSIDAD MILITAR NUEVA GRANADA
FACULTAD DE RELACIONES INTERNACIONALES ESTRATEGIA Y SEGURIDAD
PROGRAMA DE RELACIONES INTERNACIONALES Y ESTUDIOS POLÍTICOS
BOGOTÁ D.C.

2015

Resumen

La dependencia a la tecnología en la sociedad, ha venido en constante aumento hasta el punto de formar parte en todos los ámbitos de la vida, por esta razón, se hace necesario mirar cuál es el impacto que el uso de esta herramienta puede causar a las infraestructuras críticas de una nación, entendidas como

> Aquellas instalaciones, redes, servicios y equipos físicos, y de tecnología de la información cuya interrupción o destrucción tendría un impacto mayor en la salud, la seguridad o el bienestar económico de los ciudadanos o en el eficaz funcionamiento de las instituciones del Estado y de las Administraciones Públicas *(Sánchez, 2011).*

En el presente ensayo de una forma descriptiva, se determinará cuál es el impacto que puede causar un ciberataque a la infraestructura crítica esencialmente al sector de las tecnologías de la información y las comunicaciones (TIC) teniendo en consideración que de esta depende el funcionamiento adecuado de las demás infraestructuras.

Es imposible imaginar el número de consecuencias que un ciberataque puede generar en la infraestructura crítica de un Estado, afectando una sociedad y por ende al correcto funcionamiento de un país. Paralelamente al daño causado, este generará una serie de efectos secundarios los cuales al igual que los primarios, serán de difícil evaluación; sin embargo, en ambos casos el factor común es la tecnología, la dependencia a esta herramienta hace que las consecuencias tengan un efecto dominó. En el evento que la infraestructura crítica, para este caso de análisis las TIC, reciba un ciberataque no solo producirá un daño primario en este sector, si no que a su vez afectara otros sistemas vítales como el sector petroquímico, energético, de la salud, transporte, defensa, medio ambiente, gobierno, industria química, hídrico, financiero y tributario, alimentos, educación y minero, trayendo grandes efectos para el buen funcionamiento del Estado, la realización de las actividades cotidianas y en consecuencia el posible colapso de las principales ciudades.

Palabras Claves: Infraestructura crítica; Tecnologías de la información y la comunicación (TIC); Ciberataque y Seguridad.

Abstract

Dependence on technology in society has been steadily increasing to the point of being a part of all areas of life. For this reason, it is necessary to look at what impact the use of this tool can cause to the critical infrastructure, understood as

> those facilities, networks, services and hardware, and information technology whose disruption or destruction would have a greater impact on the health, safety or the economic well-being of citizens or of the effective functioning of state institutions and public administrations. (Sánchez, 2011)

This paper intends to provide a perspective on the impact that a cyber attack can have on critical infrastructure, essentially to the information and communications technology (ICT) sector, taking into account that this depends on the proper functioning of other critical points of a nation.

It is impossible to imagine the number of consequences that a cyber-attack can generate on the critical infrastructure of a state, affecting society and therefore the proper functioning of a country. Parallel to the damage caused, it will generate a number of side effects which, like the primary, will be difficult to evaluate. However, in both cases the common factor is technology, the dependence of this tool makes the consequences have a domino effect. In the event that the critical infrastructure, in this case analysis ICT, receives a cyber-attack not only a primary damage is introduced in this sector, but that in turn affects other vital systems such as the petrochemical, energy, health sector , transportation, defense, environment, government, chemical, water, finance and taxation, food, education and mining. This then has tremendous effects on the proper functioning of the state's ability to perform daily activities and consequently causes the possible collapse of major cities.

Keywords: critical infrastructure; Information and communications technology (ICT); A Cyber Attack and security.

Introducción

"El aspecto cibernético es una nueva capacidad de causar daño que no ha pasado desapercibida para los grupos terroristas y del crimen organizado, que lo han incluido como una clara alternativa para la comisión de sus atentados y delitos, respectivamente."
María José Caro (2011)

Con la evolución de la tecnología y la incorporación de ésta en todos los ámbitos de la vida, se crea un panorama globalizado de nuevas amenazas, que trae consigo mayores riesgos en las actividades sociales, industriales y comerciales tanto para las personas como para las instituciones estatales, lo que demuestra las nuevas demandas y exigencias para la protección de las actividades con plenas garantías para la seguridad. En consecuencia, la dependencia de la tecnología hace que la mayoría de las actividades sean controladas y manipuladas por éste medio, llegando a considerar la tecnología como la quinta dimensión de la guerra

> Esta dimensión asume una trascendental importancia como escenario de guerra en una era donde la globalización de las comunicaciones, determinan decisiones con efectos geopolíticos y geoestratégicos… Debemos pensar en que la guerra contemporánea se plantea el uso de cualquier medio para alcanzar un objetivo (Gaitán, 2012).

Teniendo en cuenta ésta dependencia la cual no solo está enmarcada en campos específicos de una tecnología o de la organización de un Estado, la infraestructura crítica o también conocida como sistemas vítales[1] no es ajena a este

[1] Instalaciones que son necesarias para transportar personas, útiles, energía e información, indispensables "para que una comunidad en una sociedad industrial moderna sobreviva y prospere" e" indispensables... a otras instalaciones y servicios que son críticos en un escenario de desastres, tales como hospitales, cuerpos de bomberos, y centros de operación de emergencias" (Schiff, 1984, p.p 203-205).

tipo de amenaza, dado que es imprescindible para que todas las instituciones e infraestructuras del país se encuentren en funcionamiento y constante monitoreo, teniendo en consideración que a mayor dependencia mayor será el impacto que pueda causar un ciberataque en dichas infraestructuras. En la medida que una nación no tenga la capacidad de hacerle frente a esta nueva amenaza, algunos autores consideran que una nación es frágil y por ende vulnerable, demostración típica que tan grande puede estar expuesto su heartland[2]. Esta vulnerabilidad tiene su fundamento en el internet y el uso de la tecnología, el cual ha permitido que las amenazas sean más fáciles de ejecutar y de llevar a cabo sin que el enemigo sea detectado, en consecuencia la seguridad de estos sistemas vítales no sólo depende de cuidar el área o espacio en el que se encuentran ubicadas si no de minimizar cualquier riesgo o vulnerabilidad que presentan los sistemas.

Es por eso que el presente trabajo tiene como objetivo determinar, cuál es el impacto que puede causar un ciberataque a la infraestructura crítica esencialmente al sector de las tecnologías de la información y las comunicaciones (TIC) teniendo en consideración que de esta depende el funcionamiento adecuado de las demás infraestructuras.

Asimismo se quiere analizar el impacto que ha tenido el fenómeno de las nuevas guerras (término acuñado por Mary Kaldor) y el periodo de la Guerra Fría en el conflicto armado colombiano. Posteriormente se pretende mostrar la importancia del sector de las tecnologías de la información y las comunicaciones en Colombia, para que esta llegue a ser considerada un blanco de ataque y por último se mencionará algunos de los casos más recientes de ciberataque realizados en Colombia.

[2] Para Mackinder el Corazón o Heartland de un Estado es la zona más sensible y la que da vida a la Nación, trayendo como consecuencia la muerte en caso de desaparecer o ser paralizado por las fuerzas de otros Estados. Es considerada la zona más densamente poblada, con la más compacta red de vías de comunicación y transporte, dotada de grandes recursos naturales y donde se ubican los poderes directivos del Estado. Es en esta área donde se concentra la mayor capacidad, cultural, económica, política y militar.

A partir de los atentados del 11 de septiembre, seguido de los de Londres y Madrid, ha surgido un nuevo escenario en la seguridad global, el cual plantea nuevos retos multidisciplinares que son difíciles de resolver por los medios tradicionales. De esta manera los Estados se han visto obligados a tomar medidas drásticas en la protección cibernética de sus infraestructuras críticas, pues de lo contrario las vulnerabilidades y amenazas serán difíciles de contrarrestar, trayendo grandes consecuencias no sólo para el buen funcionamiento de la nación, si no el probable colapso de las principales ciudades.

En términos generales es necesario que para poder salvaguardar la seguridad de estos sistemas vítales, dicho concepto sea reestructurado, dado que no sólo la seguridad depende desde el punto de vista tradicional, sino que tiene que involucrarse el concepto de ciberseguridad. Desde una definición estatal la ciberseguridad es entendida como "*la capacidad del estado para minimizar el nivel de riesgo al que están expuestos sus ciudadanos ante amenazas o incidentes de naturaleza cibernética" (Consejo Nacional de Política Económica y Social 3701, 2011, p.39)*, definición que debe extenderse también a la protección de las infraestructuras críticas ante cualquier ciberataque o ciberamenaza.

EL IMPACTO DE LAS NUEVAS GUERRAS Y LA GUERRA FRÍA EN COLOMBIA.

Según lo expuesto por Mary Kaldor en su libro titulado “Las Nuevas Guerras: violencia organizada en la era global”, se puede decir que en 1991 con el fin de la Guerra Fría se terminó el período de la bipolarización del mundo en sus dos ideologías la capitalista y la comunista, con estas ideologías se dio por acabada la política de contención que tenían las dos superpotencias, en las cuales se desarrollaron conflictos internos con el único objetivo de desestabilizar al oponente, al culminar este periodo (1947-1991) quedaron países totalmente militarizados y devastados tras los fuertes enfrentamientos internos. Sin embargo, la ideología comunista siguió permeando su intención en casi la mayoría de países del mundo con la única intención de buscar el poder por la vía política.

Colombia al igual que otros países en Latinoamérica no fue ajeno a este fenómeno, La Guerra Fría dejó su huella, manifestada en más de 50 años de violencia librando un conflicto armado interno con grupos insurgentes que dicen ser de la corriente comunista, como es el caso del grupo de Las Fuerzas Armadas Revolucionarias de Colombia (FARC) y el Ejército de Liberación Nacional (ELN), reflejado en constantes enfrentamientos con las Fuerzas Armadas del país. La mayor preocupación recae en los estragos de la guerra que no sólo están afectando el curso de las funciones del Estado si no que en la mayoría de los casos está acabando o marginando a la población civil.

De acuerdo a lo anterior, nace de esta manera nuevos conceptos y definiciones, como los descritos por Mary Kaldor en su libro, los cuales surgen con el desgaste de la autonomía del Estado y su pérdida de legitimidad, lo que conlleva a tener constantes conflictos armados caracterizados por la violencia organizada y la violación de los Derechos Humanos, tal como sucede en el caso colombiano. Por otra parte, la autora hace referencia a las guerras virtuales y del ciberespacio, que no son más que otro tipo de guerra que forman parte de la revolución de las relaciones

sociales de la guerra producto de la globalización y el desarrollo tecnológico. Igualmente, señala que unas de las características de las nuevas guerras es la forma en cómo esta se desarrolla y los medios empleados para llevarlas a cabo, mientras para Mary Kaldor (2001) la guerra convencional tenía como fin capturar el territorio por medios militares, las nuevas estrategias bélicas aprovechan la experiencia tanto de la guerrilla como de la lucha contrarrevolucionaria, en donde el territorio se captura por medio del control político de la población, y no a través de los medios militares.

Desde otra perspectiva, autores como Rico-Bernabé en su libro *El mantenimiento de la paz ante los retos de las nuevas guerras,* define los nuevos conflictos con una posición diferente,

> La naturaleza de los conflictos armados contemporáneos, en los que los ejércitos regulares juegan un papel secundario o bien han de enfrentarse con grupos irregulares (guerrillas, mafias, paramilitares, etc), ha influido decisivamente sobre la manera de gestionar dichos conflictos, ya que ni la diplomacia convencional ni los métodos militares tradicionales parecen estar adaptados a las estrategias de combate y de terror que se producen en la mayoría de estos conflictos, que casi su totalidad son de carácter interestatal (2002, p.8).

En relación a este nuevo concepto se observa que para el caso colombiano el concepto de “las nuevas guerras” no es nada extraño, más bien es un término nuevo para países desarrollados como Estados Unidos, pues Colombia desde hace más de 50 años vive luchando por acabar un conflicto armado interno, que lo único que le ha dejado a la sociedad es la violación constante de los Derechos Humanos y la destrucción de sus recursos humanos. Dentro de esta violencia desmedida por estos grupos armados al margen de la ley (GAML) se identifica un hecho singular y común que no obedece a una práctica con fines políticos o económicos y es el ataque a las infraestructuras críticas del país. Un ejemplo dentro de muchos en Colombia es el ataque con explosivos realizado el 17 de junio de 2015 por las FARC al oleoducto

Caño Limón-Coveñas, en donde el derrame del crudo afecto gran parte del agua del rio Catatumbo dejando a la población de la vereda Filo Guamo sin poder consumir de esta agua y causando así grandes daños a los recursos naturales del país y un daño irreparable al ecosistema.

De esta manera el terrorismo ha encontrado en los ataques a las infraestructuras críticas una herramienta para lograr sus fines. En Colombia una de las infraestructuras más atacadas por parte de los grupos armados al margen de la ley (GAML) es la petrolera, como se evidencia en el artículo Ejército Nacional de Colombia protege infraestructura petrolera contra las FARC

> Entre enero y el 30 de junio de 2014, presuntos terroristas cometieron 64 ataques a instalaciones petroleras a lo largo del país, según la Asociación Colombiana de Petróleo (ACP), estos ataques cuestan a la industria petrolera más de US$460 millones en ventas perdidas (…) El 80% de los ataques han tenido lugar en los departamentos de Arauca, Norte de Santander y Putumayo (Pelcastre, 2014).

Es claro que para una organización terrorista la afectación a infraestructuras críticas constituye una blanco rentable pues logra de manera directa impactar la población y el funcionamiento adecuado del Estado. En consecuencia y como mecanismo de respuesta el gobierno ha tomado la medida de desplegar un mayor número de tropas en las zonas donde se encuentran ubicadas estas infraestructuras, pero no se ha tenido en cuenta que con el uso de la tecnología estos sistemas vítales se encuentran enfrentados a unas nuevas ciberamenazas o ciberataques, que pueden constituirse en una forma alterna para que los grupos armados al margen de la ley (GAML) intenten alterar el funcionamiento de la infraestructura sin necesidad de ser detectados.

De igual manera, se observa que el fenómeno de las nuevas guerras está rompiendo con el paradigma del dilema de la Seguridad Nacional Clásica, pues ya no sólo es suficiente con proteger o cuidar las zonas que se encuentran en constante peligro de ser atacadas, si no que estas nuevas amenazas están siendo propagas por medio de la tecnología, la cual permite que sean mucho más fáciles y rápidas de ejecutar sin que el enemigo sea detectado. Desde otro lado, es evidente que cierto número de actos delictivos en la red se pueden perseguir, pero estos en cualquier momento y lugar pueden volver a presentarse, generándose así ciberamenazas latentes.

Como ejemplo de estas nuevas guerras Kaldor utiliza la guerra de Kósovo porque

> En primer lugar, fue una guerra librada en nombre del «nuevo nacionalismo». Algunos podrían decir que el argumento de los «antiguos odios» es mucho más fuerte en Kósovo que en Bosnia (…) En segundo lugar, los métodos de la guerra representaron el perfeccionamiento de las técnicas desarrolladas en Croacia y Bosnia, la estrategia de controlar el territorio mediante el desplazamiento de la población. La violencia se dirigió principalmente contra los civiles (…) Por último, el conflicto Kósovo fue también un ejemplo característico de nueva economía de guerra (p.p. 197-202).

LA IMPORTANCIA DEL SECTOR DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIÓNES EN COLOMBIA.

En la actualidad la sociedad ha demostrado una dependencia a la tecnología hasta tal punto de controlar todos los ámbitos de la vida. Este tipo de dependencia ha hecho que los gobiernos y para el caso colombiano designen el Ministerio de las Tecnologías de la Información y la Comunicación más conocida como TIC, con la función de "diseñar, adoptar y promover las políticas, planes, programas y proyectos del sector de las Tecnologías de la Información y las Comunicaciones" (2015), pero esta entidad no sólo cumple con esas funciones, si no que desde un punto de vista más analítico, es el que se encarga de velar por el buen funcionamiento de las infraestructuras críticas que conforman el país, cosa que la hace más vulnerable ante cualquier ciberamenaza o ciberataque.

En cuanto a ciberamenaza se puede decir que ésta es entendida como

> El grado de certeza que poseen los Estados o particulares, que sus infraestructuras críticas o sistemas vítales empleados para el desarrollo de la vida en sociedad, presentes en el ciberespacio, pueden ser atacados por organizaciones estales encubiertas o no, por organizaciones particulares privadas o por individuos interesados en hacer daño (Stel, 2014, p. 137).

Mientras ciberataque para el mismo autor "*es aquel ataque ejecutado en el ciberespacio, declarado o no, dirigido contra una organización estatal, organizaciones y empresas privadas o individuos en particular, para producir un efecto calculado aunque en algunos casos pueden tener resultados impredecibles e imponderables"* (2014, p.138), es de resaltar que este tipo de ataques no tienen un lugar específico y pueden llegar a afectar áreas interrelacionadas como el caso de las infraestructuras críticas.

De igual manera es importante hacer énfasis en la diferencia existente entre una guerra electrónica y una ciberguerra, ya que estos conceptos son totalmente independientes, entendiendo la guerra electrónica como

> La denominación general que comprende las acciones adoptadas para buscar, interceptar, identificar y/o ubicar fuentes de energía irradiadas con el fin de obtener un reconocimiento inmediato de una amenaza. Así pues, los sistemas de contramedida suministran una fuente de información requerida para acción inmediata que incluye contramedidas electrónicas, acciones de evasión, localización del blanco y otro empleo táctico de las fuerzas (García, p.3).

Mientras que el concepto de ciberguerra es definida por Prabir Purkayastha como

> Ataques en el ciberespacio que traspasan un umbral determinado. Un enfoque para la definición de la ciberguerra sería en términos del daño físico que un ataque cibernético causaría en el mundo real. El ataque, por parte de un Estado contra otro, utiliza el software o código destinado a impedir el funcionamiento (o el mal uso) de una red informática esencial, y así dañar la infraestructura crítica, o causar daño físico a la propiedad o a las personas –incluyendo la pérdida de la vida–, o a ambas. En esta definición, la ciberguerra siempre implica un actor estatal, no es el trabajo de un grupo o un individuo (2015).

Por ende la diferencia de los dos conceptos radica, en que la guerra electrónica tiene como fin impedir el uso militar del espectro electromagnético por parte del enemigo y su vez poder aprovecharlo en beneficio propio, teniendo en cuenta que este es un campo netamente utilizado por militares, mientras que la ciberguerra se desarrolla por medio del ciberespacio convirtiéndolo en un campo más difuso, ya que en él se encuentran inmersos diferentes interconexiones bien sean civiles o del

Estado, permitiendo que realizar un ciberataque a la infraestructura critica sea mucho más fácil.

La tecnología hoy en día juega un papel muy importante en la sociedad pues permite el intercambio de información, facilita la comunicación, permite eliminar las fronteras tradicionales entre los diferentes Estados para generar una mayor cercanía entre las personas y permite controlar cualquier proceso o funcionamiento de las máquinas a las cuales se encuentran inmersas. Pero así como lo mencionan Guerra y Sánchez en su libro *Bioética y Tecnoética: Alternativas para un mundo deshumanizado*

> La normatividad y legislación asociada al uso de la tecnología encuentra sus mayores obstáculos en la jurisdicción competente y la ley aplicable como conceptos geográficamente marcados. Al no tener las TIC una ubicación espacial y ser esencia transfronterizas, la ley encuentra sus limitaciones dentro de un concepto territorial (2012, p.83).

Esta condición hace que los Estados deban de preocuparse en encontrar posibles soluciones a los ciberataques o ciberamenazas a los cuales se encuentran expuestos a diario, y así de alguna manera poder proteger los contenidos o sistemas que eventualmente puedan perjudicar la seguridad del Estado y sus ciudadanos, en razón a lo anterior en un estudio (Reporte de Seguridad Cibernética e Infraestructura Crítica de las Américas) realizado por la Organización de los Estados Americanos, se menciona que Colombia es uno de los países pioneros en la región en concentrar todos sus esfuerzos en cuanto a ciberseguridad[3] se refiere, pero eso se debe según el estudio porque

> Colombia ha estado luchando contra las Fuerzas Armadas Revolucionarias de Colombia (FARC) durante varias décadas, una lucha que hace que las Fuerzas Militares y la Policía, en coordinación

[3] Conjunto de acciones de carácter preventivo que tienen por objeto el asegurar el uso de las redes propia y negarlo a terceros. Tomado de http://www.cari.org.ar/pdf/ciberdefensa_riesgos_amenazas.pdf

> con el sector privado, defiendan y protejan la infraestructura crítica física y virtual del país. Por tanto, en la etapa final de su Política Nacional de Ciberseguridad y Ciberdefensa (CONPES 3701/2011), se han formado grupos de trabajo y se incluyen a las Instituciones del Gobierno Nacional (Ministerio de Defensa Nacional, MINTIC, la Policía Nacional, etc.) y a las organizaciones del sector privado (representantes de los sectores de energía y comunicaciones, administradores de los dominios .co, universidades, etc.) para crear un marco serio y coordinado que busca proteger las infraestructuras críticas del país (Organización de los Estados Americanos, 2015, p. 17).

De acuerdo a lo anterior y como mecanismo de respuesta se resalta que a partir del 2011 Colombia creó una Política Integral de Ciberseguridad y Ciberdefensa[4] por medio del CONPES 3701, la cual se fundamenta en tres pilares esenciales: implementar la institucionalidad apropiada, fomentar programas de capacitación especializada y fortalecer la legislación y cooperación internacional, tiene como objetivo identificar, priorizar y clasificar la infraestructura crítica del país, también será una plataforma que permita conectar a las diferentes organizaciones de seguridad con el propósito de que éstas brinden una protección efectiva a los sistemas vítales y como última medida se encargará de la planeación y creación de la Estrategia Nacional de Defensa de la infraestructura crítica.

Esta Política Nacional de Ciberseguridad contará con un modelo de coordinación capaz de afrontar estas nuevas amenazas, conformada por el Grupo de Respuesta a Emergencias Cibernéticas de Colombia (ColCERT), el Centro Cibernético Policial y el Comando Conjunto Cibernético (ver anexo1), según el Consejo Nacional de Política Económica y Social 3701 (2011) "*La Comisión Intersectorial encargada de fijar la visión estratégica de la gestión de la información, así como de establecer los lineamientos de política respecto de la gestión de la infraestructura tecnológica*

[4] Conjunto de acciones de defensa activas pasivas, proactivas, preventivas y reactivas para asegurar el uso propio del ciberespacio y negarlo al enemigo o a otras inteligencias en oposición. Tomado de http://www.cari.org.ar/pdf/ciberdefensa_riesgos_amenazas.pdf

(hardware, software y comunicaciones), información pública y ciberseguridad y ciberdefensa" (p.21). Esta nueva estrategia se encargará de involucrar a todos los sectores afectados como las empresas estatales, empresas privadas, la academia y la sociedad civil, donde se busca establecer un mecanismo de cooperación entre la Policía Nacional encargados de la ciberseguridad en el país apoyados por las Fuerzas Armadas, mientras que estos últimos se encargaran de todo lo relacionado con la Ciberdefensa de Colombia apoyados igualmente por la Policía Nacional.

Respecto a la implementación de esta estrategia se evidencia un gran avance, primero con la creación de la comisión interestatal, segundo con la campaña de sensibilización llevada a cabo por el Ministerio de la Información y las Telecomunicaciones (TIC) denominada "En TIC confió[5]", adicionalmente la inclusión de nuevos cursos de ciberseguridad en el Servicio Nacional de Aprendizaje (SENA), la nueva cátedra de Defensa Nacional Digital de las Escuelas de Formación de las Fuerzas Militares, y en cuanto a la legislación

> El Ministerio TIC, por medio del Manual 3.0 de Gobierno en Línea, generó una serie de directrices en temas de seguridad de la información basada en estándares internacionales, que deberán ser implementadas por las entidades del sector público. Por su parte, la Comisión de Regulación Colombiana se encuentra elaborando la regulación de los Proveedores de Servicios de Internet (ISP, por sus siglas en inglés) para conservar los dominios de uso de internet. (Cámara Colombiana de Informática y Telecomunicaciones y Fedesarrollo, 2014, p. 8)

En virtud de lo expuesto anteriormente se puede decir que, el sector de las tecnologías de la información y las comunicaciones (TIC) se constituye en una infraestructura crítica importante, pues en el transcurso de este escrito se ha podido evidenciar la dependencia que los demás sistemas vítales han generado de ésta, de

[5] En "TIC confío" es la Política Nacional de uso responsable de las TIC del Plan Vive Digital del Ministerio TIC, mediante la cual se quiere promover la confianza y seguridad en el uso de las telecomunicaciones en Colombia. Tomado de: http://www.fedesarrollo.org.co/wp-content/uploads/TIC-Noviembre-2014_Web.pdf

allí resalta la importancia de hacer énfasis en que se entiende por una infraestructura crítica, según el Plan Nacional de Protección de Infraestructuras Críticas Española (2009) éstas se entiende como

> Aquellas instalaciones, redes, servicios y equipos físicos y de tecnología de la información cuya interrupción o destrucción tendría un impacto mayor en la salud, la seguridad o el bienestar económico de los ciudadanos o en el eficaz funcionamiento de las instituciones del Estado y de las Administraciones Públicas (Baró y Vallejo, 2010, p.6).

En consecuencia, la definición o concepto de infraestructura crítica trae consigo una multiplicidad de sectores afectados como lo son el sector petroquímico, el energético, el de la salud, el transporte, el defensa, medio ambiente, gobierno, industria química, hídrico, financiero y tributario, alimentos, educación, minero y el de las tecnologías de la información y la comunicación (TIC) objeto central de este análisis. Sin embargo una característica común de dichos sectores se encuentran en la interconexión gracias al empleo de la tecnología, lo que genera que una falla en alguno de ellos pueda afectar a los demás sectores, es decir, si el sector TIC presenta falencias, este generara un efecto dominó y estas fallas alcancen a los demás sectores anteriormente mencionados.

Pero en realidad la pregunta es ¿Por qué este sector es tan importante para el buen funcionamiento del Estado y de las actividades cotidianas de la sociedad?, es significativo mencionar que este sector está a cargo del Ministerio de Tecnologías de la Información y las Comunicaciones, el cual es el encargado de promover “el acceso y uso de las TIC a través de la masificación, el impulso a la libre competencia, el uso eficiente de la infraestructura y en especial fortalecer la protección de los derechos de los usuarios” (Ministerio de Tecnologías de la Información y las comunicaciones, 2015).

Según El Tiempo en su artículo denominado *¿Qué tanto aporta la industria TIC a la economía nacional?* es evidente que debido a la dependencia tecnológica que se tiene en el país, el sector de las TIC en los últimos años ha logrado tener un crecimiento significativo y a su vez jugar un papel primordial para potenciar la productividad de la mayoría de los sectores económicos, lo que le ha permitido convertirse en uno de los sectores que más aportan a la economía del país tal como lo mencionan

> Con relación a las 53 actividades que le aportan a la economía del país, la actividad correo y telecomunicaciones se encuentra en el noveno lugar dentro del escalafón de las actividades económicas que más le aportan al producto interno bruto, con una participación del 3,13 por ciento (…) adicionalmente las telecomunicaciones es la industria que más externalidades positivas genera en la economía donde se resaltan: generación de empleo, aumento de productividad, incremento del PIB, seguridad, acceso a educación e inclusión social entre otros" (El Tiempo, 2015).

Por lo anterior el sector de las TIC se convierte no solo en un objetivo más sino en un blanco estratégico a ser atacado, pues de ella no sólo depende el buen funcionamiento de las redes de comunicación, si no toda la infraestructura crítica que forma parte del Estado. La característica y funcionabilidad de las mismas sumado al empleo de la tecnología su manejo y monitoreo por medio de un sistema en cascada[6], que hace que una vulnerabilidad o ataque en una de ellas se extienda a las demás en un efecto en cadena no sólo afectando a dichas infraestructuras, si no trayendo grandes consecuencias para la seguridad, el buen funcionamiento del Estado y por supuesto una interrupción en las actividades cotidianas de los ciudadanos y de las empresas.

[6] Se define como la configuración donde la salida de un controlador de realimentación es el punto de ajuste para otro controlador de realimentación, por lo menos. Más exactamente, el control de cascada involucra sistemas de control de realimentación o circuitos que estén ordenados uno dentro del otro. Tomado de: https://dinamicaycontrol.files.wordpress.com/2012/03/resumen-control-cascada.pdf

CASOS DE CIBERATAQUES EN COLOMBIA.

Antes de entrar en detalles sobre los ciberataques realizados a algunas infraestructuras críticas colombianas, es indispensable tener en cuenta que muchos de estos delitos informáticos no se encuentran regulados, debido al difícil seguimiento que esto suponen por el uso del internet, tal como lo mencionan las autoras Guerra y Sánchez (2012) en un apartado de su libro

> El código de derecho penal colombiano expedido con la Ley 599 de 2000, no hace referencia expresa a los delitos tecnológicos o informáticos como tales, pero algunas de sus normas podrían conceptualizarlo como: "aquellas conductas que recaen sobre herramientas informáticas propiamente, llámense programas, ordenadores, etc.; como aquellas que valiéndose de estos medios lesionan otros intereses jurídicamente tutelados como son la intimidad, el patrimonio económico, la fe pública, etc" (p.p. 92-93).

Por otra parte, el 5 de enero de 2009 el Congreso de la República aprobó la Ley 1273 "De la Protección de la información y de los datos", donde se crean nuevos delitos informáticos con pena de prisión hasta de 120 meses y multas de alrededor de los 1500 salarios mínimos para las personas que cometan actos como: Acceso abusivo a un sistema informático, obstaculización ilegitima de sistema informático o red de telecomunicación, interceptación de datos informáticos, daño informático, uso de software malicioso, violación de datos personales, suplantación de sitios webs para capturar datos personales, hurto por medios informáticos y semejantes, transferencia no consentida de activos, entre otros. Lo anterior con el fin de poder preservar y proteger integralmente los sistemas que utilizan las tecnologías de la información y de la comunicación (Ley 1273, 2009, p.p. 1-3).

Teniendo en cuenta lo anteriormente mencionado, y para el caso particular de Colombia se han presentado dos ciberataques recientes:

1. Caso de Anonymous y su ataque a las páginas webs de las entidades colombianas: Este caso catalogado como ciberactivismo, dado que son personas dedicas a cuestiones socio-políticas que emplean las redes sociales para atraer seguidores e informar cada una de sus acciones, para este ejemplo se utiliza youtube (hacer lobby) y Twitter. Adicionalmente se clasificó también como hacktivismo, pues sus prácticas persiguen el control de ordenadores o sitios web para promover su causa, como sucedió en el caso de Colombia, en donde estos a través de su cuenta de twitter invitaron a las personas a realizar un ingreso masivo a la página del Ministerio de Educación, con el objetivo de colapsarla pues no estaban de acuerdo en que dicha entidad buscara atraer capitales privados a las universidades, posteriormente el ataque se extendió a otras entidades como el Ministerio de Defensa, El Senado y La Presidencia conllevando a que éstas fueran suspendidas temporalmente.

Otro caso de este grupo fue un ciberataque, que se llevó a cabo a raíz de la muerte del grafitero Diego Becerra presuntamente a manos de la Policía Nacional, esto ocasionó que anonymous por medio de su red social se atribuyera un ataque a la página oficial de la Policía Nacional como rechazo a la muerte del joven argumentando **“Familiares del compañero Grafitero asesinado sepan que anonymous está con ustedes y no vamos a permitir que el silencio y la impunidad reine”** (El Espectador, 2011)**,** este caso es conocido como “Operación emergencia en contra de los falsos positivos”.

2. La segunda ciberataque empezó a raíz de los diálogos de paz realizado en la Habana, en el 2014 se dieron a conocer graves acusaciones en contra del “Hacker” Andrés Sepúlveda, por realizar actividades de ciberespionaje, acceso abusivo a un sistema informático, uso de software malicioso y la violación a datos personales, pues se encontró culpable por realizar interceptaciones a miembros del equipo negociador de la Habana. Se menciona que Sepúlveda fue contratado por grupos políticos interesados en asuntos de Seguridad

Nacional, adicionalmente se vincula con la fachada de andrómeda, en la cual se estarían realizando operaciones ilegales de espionaje como interceptación telefónica y de hackeo de correos electrónicos.

En cuanto a ciberespionaje, referido en el artículo *Riesgo Inminente* publicado por la revista Dinero (2014) en Colombia éste es un delito frecuente, ya que a menudo los hackers emplean ingeniería social (técnica que permite obtener información confidencial a través de la manipulación de las víctimas), con el objetivo de poder clonar y robar todo el dinero que tienen en sus cuentas bancarias, pero esto no solo se utiliza con las personas si no también con las empresas, que por medio de internet mueven altos flujos de dinero como fue el caso del desfalco cibernético más oneroso de la historia del país, en donde un grupo de delincuentes lograron sustraer de las cuentas bancarias de una compañía alrededor de $7.500 millones de pesos colombianos.

En Colombia durante el 2014 se realizaron aproximadamente 205 capturas por hurto en medios informáticos, relacionados con clonaciones de tarjetas, software malicioso o infiltración directa a las empresas afectadas, pero según estudios realizados por la Policía Nacional se cree que la mayoría de estos casos se presentan porque los usuarios no siguen instrucciones de seguridad y la constante exposición a redes sociales que les permite a los atacantes practicar ingeniería social y aprovecharse de las debilidades de seguridad y atacar las cuentas.

A pesar de que los casos presentados anteriormente son preponderantes en la vida política o mediática, se evidencia que Colombia hasta el momento no ha sufrido graves ciberataques a sus infraestructuras críticas por parte de grupos armados al margen de la ley (GAML), es por eso que se procura crear una alerta frente a un futuro cercano y como los grupos terroristas y las nuevas amenazas pueden cambiar su estrategia de ataque, es decir, que éstos no se lleven a cabo en el espacio geográfico en el cual se encuentra ubicada la infraestructura, si no que sean atacadas por medio de la tecnología, como ha sucedido en Estados Unidos en donde para el 2007 una red

informática del Pentágono sufre un ataque lanzado por Hackers desde China convirtiéndose en uno de los ciberataques de más éxito al Departamento de Defensa de éste país. Otro caso conocido es el de Estonia, el cual culpa a las autoridades de Rusia de generar diversos ataques que afectaron a medios de comunicación, bancos y diversas entidades e instituciones gubernamentales, generando una parálisis nacional.

Como se ha venido desarrollando, la dependencia a la tecnología hace a las personas e instituciones del Estado más sensibles a diferentes ciberamenazas y los exponen a constantes vulnerabilidades en los sistemas informáticos. Por otra parte no se puede desconocer que la principal vulnerabilidad siempre serán los seres humanos, los cuales no siempre toman las medidas de seguridad necesarias para proteger su información, cosa que no solo sucede dentro de la población civil si no también dentro de las organismos del Estado, en donde no aplican la ciberseguridad y ciberdefensa para proteger el tipo de información clasificada.

Aunque en países como Colombia se han presentado ataques a la infraestructura crítica por parte de grupos armados al margen de la ley (GAML), no se observa que estos sistemas vítales hayan sido ciberatacados por parte de éstos, más bien las acciones de ciberataque en Colombia han sido netamente con fines políticos y mediáticos donde los mismos actores políticos tradicionales o emergentes se afectan mutuamente. Es clara la necesidad de tomar las medidas drásticas para salvaguardar la ciberseguridad de estas infraestructuras, pues debido al conflicto armado interno que se vive en el país, grupos armados al margen de la ley (GAML) como las FARC y el ELN pueden cambiar sus estrategias de ataque, pues como se ha mencionado en el transcurso de este escrito, los ciberataques son mucho más rápidos y la detección del enemigo es más complicada, en razón a lo expuesto no es extraño que los grupos ilegales traten de afectar al Estado y a la población civil por otros medios.

La OEA en sus últimos estudios realizados al respecto exponen que los ciberataques en América Latina podrían aumentar gradualmente dentro de la 10 a 15

años, en donde los principales puntos afectados serían las infraestructuras críticas, debido a que los "*Grupos que antes se centraban en el robo de información ahora están más interesados en la destrucción y sabotaje de infraestructuras claves de gobiernos y grandes instituciones privadas*" (Redacción Tecnología, 2015).

CONCLUSIONES.

Se puede resaltar que el impacto de las nuevas guerras y el periodo de la Guerra Fría, ha dejado grandes consecuencias para el país, pues en el caso de las nuevas guerras se evidencia que estas ya no sólo se llevaran a cabo en un espacio tridimensional (tierra, mar y aire), si no que ésta ha ampliado su escenario al ciberespacio, el cual es por naturaleza dinámico y de cambios constantes llegando a considerarse como la quinta dimensión de la guerra, mientras que la Guerra Fría dejado sus huellas con la creación de grupos armados al margen de la ley (GAML). La combinación de estos dos factores hará que estos grupos en un futuro cercano puedan cambiar sus estrategias de ataque.

Hay que resaltar que la implementación de la tecnología en la infraestructura crítica hace que existan constantes amenazas y vulnerabilidades y es ahí donde radica la importancia del sector de las tecnologías de la información y las comunicaciones, debido a que de ella depende la correcta manipulación y funcionamiento de los demás sistemas vitales, ya que estas se encuentran interconectadas por medio de un sistema en cascada, lo que hace que el sector de las TIC se convierta en un punto blanco de ataque.

Para finalizar se puede decir que aunque los casos de ciberataques expuestos en el transcurso de la investigación no son llevados a cabo por grupos armados al margen de la ley (GAML), esto no quiere decir que grupos como las FARC, el ELN, las BACRIM (Bandas Criminales Emergentes), entre otras, puedan cambiar sus estrategias de ataque no solo afectando el correcto funcionamiento del Estado sino a la población civil, debido a que sus actividades cotidianas se verían suspendidas llegando a generar el colapso de las principales ciudades.

RECOMENDACIONES.

Es necesario que para salvaguardar la seguridad de las infraestructuras críticas no sólo en el espacio geográfico en el que se encuentran ubicadas si no también la de sus sistemas operativos, el gobierno trabaje en coordinación con el sector privado, pues en la mayoría de los casos el buen funcionamiento de estos sistemas vítales depende de las empresas privadas. Adicionalmente se deben crear políticas públicas que ayuden a mantener la Seguridad y Defensa tanto del territorio Nacional como la de los ciudadanos, ya que si no existen instituciones o normas que regulen este tipo de actos delictivos las consecuencias serán mayores.

Para poder mantener la seguridad de las infraestructuras criticas especialmente la del sector de las tecnologías de la información y las comunicaciones, es importante que la Política Nacional de Ciberseguridad y Ciberdefensa sea actualizada constantemente y que se llegue a ejecutar en todos los campos que puedan afectar a las infraestructuras críticas, pues es fundamental que se realice una revisión exhaustiva de la infraestructura tecnología que permiten el buen funcionamiento de los sistemas vítales y de la información sensible, para poder establecer los protocolos necesarios para la administración adecuada de la seguridad de las tecnologías de información y así de alguna manera poder contrarrestar estas amenazas.

Es importante que para mitigar los riesgos o vulnerabilidades de una ciberamenaza o un ciberataque se capacite a las personas que operan las infraestructuras críticas, porque como se mencionó el principal punto de vulnerabilidad y de riesgo son los mismos seres humanos, es por eso que se hace necesario que estas personas conozcan todo lo relacionado con la ciberseguridad y la ciberdefensa en donde puedan recibir constantes capacitaciones, pues todos los días están surgiendo nuevas amenazas. Para lo anterior se deben tomar medidas como: actualizar el software antivirus del sistema operativo, actualizaciones de los navegadores de internet, utilizar contraseñas de alta protección, descargar software de páginas conocidas y autorizadas, no abrir archivos adjuntos de correos no solicitados.

GLOSARIO.

- **Centro Cibernético Policial:** Estará encargado de la ciberseguridad del territorio colombiano, ofreciendo información, apoyo y protección ante los delitos cibernéticos. Desarrollará labores de prevención, atención, investigación y judicialización de los delitos informáticos en el país, informando en su página web sobre vulnerabilidades cibernéticas. Recibirá y atenderá los lineamientos nacionales en ciberseguridad y trabajará de forma coordinada con el colCERT (CONPES 3701, 2001, p. 25).

- **Ciberespacio:** Espacio virtual que engloba todos los sistemas TIC, tanto sistemas de información como sistemas de control industrial. El ciberespacio se apoya en la disponibilidad de Internet como red de redes, enriquecida con otras redes de transporte de datos (Centro Criptológico Nacional, 2015, p. 208).

- **Ciberespionaje:** Se puede definir como el conjunto de actividades de espionaje llevadas a cabo en el ciberespacio o utilizando el ciberespacio como medio (Centro Criptológico Nacional, 2013, p. 210).

- **Cibernética:** Estudio de las analogías entre los sistemas de control y comunicación de los seres vivos y los de las máquinas; y en particular, el de las aplicaciones de los mecanismos de regulación biológica a la tecnología (Real Academia de la Lengua Española, ___)

- **Comando conjunto cibernético:** Estará en cabeza del Comando General de las Fuerzas Militares, quien podrá delegar sus funciones dentro de las Fuerzas Militares dependiendo de las especialidades existentes en el sector. Este deberá prevenir y contrarrestar toda amenaza o ataque de naturaleza cibernética que afecte los valores e intereses nacionales (CONPES 3701, 2001, p. 24)

- **Conflicto armado interno**: Un conflicto armado interno se presenta al interior de un país cuando existen fuerzas armadas, diferentes a las gubernamentales, que se

oponen al gobierno o a otras fuerzas armadas por motivos étnicos, políticos o religiosos (Arango, 2011).

- **ELN:** Sigla utilizada para designar al Ejército de Liberación Nacional, es el segundo grupo guerrillero con más hombres en sus filas después de las FARC, con una ideología marxista-leninista, surge en la década del sesenta de la mano de la revolución cubana de Fidel Castro. En 1965 incursiona en la guerra de guerrillas y en ese mismo año crea su primer frente (El Tiempo. 2014).

- **FARC:** Es aquella que se utiliza para designar a las Fuerzas Armadas Revolucionarias de Colombia, una asociación paramilitar ilegal y no reconocida por el Estado colombiano, con una ideología marxista-leninista que se especializa en el secuestro, tortura y extorsión de personas tanto colombianas como extranjeras (Definición ABC, ____).

- **Grupo armado al margen de la ley:** Se entiende por grupo armado organizado al margen de la ley aquel grupo de guerrilla o de autodefensas, o una parte significativa e integral de los mismos como bloques, frentes u otras modalidades de esas mismas organizaciones que, bajo la dirección de un mando responsable, ejerza sobre una parte del territorio un control tal que le permita realizar operaciones militares sostenidas y concertadas (Medina, 2014).

- **Grupo de respuesta a emergencias cibernéticas de Colombia:** Será el organismo coordinador a nivel nacional en aspectos de ciberseguridad y ciberdefensa. Prestará su apoyo y colaboración a las demás instancias nacionales tales como el Centro Cibernético Policial - CCP y el Comando Conjunto Cibernético - CCOC. El colCERT será un grupo del Ministerio de Defensa Nacional, integrado por funcionarios civiles, personal militar y en comisión de otras entidades (CONPES 3701, 2001, p. 22)

- **Riesgo:** Estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización (Centro Criptológico Nacional, 2015, p. 756).

- **Violencia organizada:** Se llama así a la violencia que puede provenir de grupos subversivos organizados, del Estado o de parte de los militares. La tortura o la muerte violenta serían una expresión de la violencia de origen político (Errázuriz & Pedersen, 2007, p. 8).

- **Vulnerabilidad:** Debilidad o falta de control que permitiría o facilitaría que una amenaza actuase contra un objetivo o recurso del Sistema (Centro Criptológico Nacional, 2015, p. 919).

ANEXOS.

ANEXO 1.

Gráfica No. 5 Modelo de Coordinación
Fuente: Ministerio de Defensa Nacional

Fuente: Departamento Nacional de Planeación (2011). "Lineamientos de política para ciberseguridad y ciberdefensa". Consejo Nacional de Política Económica y Social. República de Colombia. P. 21.

Referencias

Actualidad. (16 de agosto de 2011). Ciberataque de Anonymous contra el gobierno colombiano. *Actualidad.* Recuperado de: http://actualidad.rt.com/ciencias/view/31368-Ciberataque-de-Anonymous-contra-gobierno-colombiano

Arango, M. (19 de mayo de 2011). Colombia. Conflicto Armado Interno y La Ley de Victimas. Recuperado de: http://www.anarkismo.net/article/19614?search_text=sinos&userlanguage=it&save_prefs=true

Ávila, T. (____). *Identificación y valoración de la vulnerabilidad al terrorismo, en infraestructura petrolera.* Bogotá, Colombia: Editorial Universidad de los Andes. Recuperado de: http://abiquim.org.br/congresso/cong_cd/fullpapers/P155672.pdf

Baker, S., Waterman, S. & Ivanov, G. (____). En el punto de mira las infraestructuras críticas en la era de la ciberguerra. *McAfee.* Madrid, España. Recuperado de: http://www.belt.es/expertos/CIP_report_final_es_fnl_lores.pdf

Baró, B. & Vallejo, E. (2010). *Protección Infraestructuras Críticas en el Port de Barcelona.* Barcelona, España. Recuperado de: http://www.uab.cat/servlet/BlobServer?blobtable=Document&blobcol=urldocument&blobheader=application/pdf&blobkey=id&blobwhere=1339655202662&blobnocache=true

Basallo, A. (2008). *Seguridad de la información y protección de Datos. Seguridad pública y protección civil.* Recuperado de: http://www.belt.es/articulos/HOME2_articulo.asp?id=5402

Cámara Colombiana de Informática y Telecomunicaciones & Fedesarrollo. (Noviembre de 2014). *Avances y retos de la defensa digital en Colombia.* Recuperado de: http://www.fedesarrollo.org.co/wp-content/uploads/TIC-Noviembre-2014_Web.pdf

Cañizares, R. (). Formación en protección de infraestructuras críticas. *Revista decana independiente de seguridad.* (416). Recuperado de: http://www.seguritecnia.es/revistas/seg/416/files/assets/common/downloads/files/seg_416_blq.pdf

Caro, M. (2011). *La protección de las infraestructuras críticas.* Instituto Español de Estudios Estratégicos. Madrid, España. Recuperado de: http://www.ieee.es/Galerias/fichero/docs_analisis/2011/DIEEEA21_2011ProteccionInfraestructurasCriticas.pdf

Carratalá, I. (____). *Cultura de seguridad en infraestructuras críticas.* Recuperado de: http://www.belt.es/expertos/HOME2_experto.asp?id=6769

Centro criptológico Nacional. (Julio de 2015). Guía de seguridad (CCN-STIC-401) Glosario y Abreviaturas. Madrid, España. Recuperado de: https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/400-guias-generales/976-ccn-cert-401-glosario-y-abreviaturas/file.html

Congreso de Colombia. (5 de enero de 2009). Ley de la protección de la información y de los datos. [Ley 1273 de 2009]. Recuperado de: http://www.mintic.gov.co/portal/604/articles-3705_documento.pdf

Consejo Argentino para las Relaciones Internacionales. (2013). *Ciberdefensa-Ciberseguridad. Riesgos y amenazas.* Argentina. Recuperado de: http://www.cari.org.ar/pdf/ciberdefensa_riesgos_amenazas.pdf

Cúcuta. (17 de junio de 2015). Miniambiente evalúa daños en región del Catatumbo por derrame de Crudo. *El Tiempo.* Recuperado de: http://www.eltiempo.com/colombia/otras-ciudades/ataque-de-la-guerrilla-al-oleoducto-cano-limon-covenas/15961936

Definición ABC. (____). Definición de FARC. Recuperado de: http://www.definicionabc.com/historia/farc.php

Dinero. (27 de noviembre de 2014). Riesgo inminente. *Revista Dinero.* Recuperado de: http://www.dinero.com/edicion-impresa/pais/articulo/crecimiento-delitos-ciberneticos-colombia/203563

El Colombiano. (27 de septiembre de 2013). TIC representa 6% del PIB. *El Colombiano.* Recuperado de: http://www.elcolombiano.com/historico/tic_representan_6_del_pib-JYEC_262478

El Espectador. (26 de septiembre de 2011). Anonymous ataca página web de la Policía en rechazo a muerte de joven grafitero. *El Espectador.* Recuperado de: http://www.elespectador.com/tecnologia/anonymous-ataca-pagina-web-de-policia-rechazo-muerte-de-articulo-302090

El Tiempo. (10 de junio de 2014). ¿Qué es el ELN?. Recuperado de: http://www.eltiempo.com/politica/proceso-de-paz/historia-del-eln/14100715

Errázuriz, C. & Pedersen, D. (Diciembre de 2007). Problemas relacionados con la violencia: Violencia Organizada. Perú. Recuperado de https://www.mcgill.ca/files/trauma-globalhealth/Modulo_05.pdf

Gaitán, A. (2012). El ciberespacio: Un nuevo teatro de batalla para los conflictos armados del siglo XXI. Bogotá, Colombia: Escuela Superior de Guerra.

García, L. (___). Guerra Electrónica. Universidad Pontificia Comillas. Madrid, España: Recuperado de: http://www.iit.upcomillas.es/pfc/resumenes/44925c439f51e.pdf

Guerra, Y. & Sánchez, A. (2012). *Bioética y Tecnoética. Alternativas para un mundo deshumanizado.* Bogotá, Colombia: Editorial Universidad Militar Nueva Granada.

La Nación. (5 de septiembre de 2007). Tensión por el ciberataque al Pentágono. *La Nación.* Recuperado de: http://www.lanacion.com.ar/940981-tension-por-el-ciberataque-al-pentagono

Martínez, R. (18 de mayo de 2007). Los "ciberataques" a Estonia desde Rusia desatan la alarma en la OTAN y la UE. *El País.* Recuperado de: http://elpais.com/diario/2007/05/18/internacional/1179439204_850215.html

Medina, J. (25 de marzo de 2014). Términos y siglas de Grupo Armado Organizado al Margen de la Ley. Recuperado de: http://www.reintegracion.gov.co/es/atencion/Lists/Trminos%20y%20Siglas/DispForm.aspx?ID=16&Source=http%3A%2F%2Fwww%2Ereintegracion%2Egov%2Eco%2Fes%2Fatencion%2Flists%2Ftrminos%2520y%2520siglas%2Fallitems%2Easpx%23InplviewHash1e41cfa2-505a-4b2c-a6c6-cebfad7606ac%3D&ContentTypeId=0x01008F9C8BC0E60EA44D8D34863E87467E3F

Ministerio de Tecnologías de la Información y las Comunicación. (____). *Historia.* Bogotá, Colombia. Recuperado de: http://www.mintic.gov.co/portal/604/w3-propertyvalue-6077.html

Ministerio de Tecnologías de la Información y las Comunicación. (____). *Ciberseguridad.* Bogotá, Colombia. Recuperado de: http://www.mintic.gov.co/portal/604/w3-article-6120.html

Ministerio de Tecnologías de la Información y las Comunicaciones. (____). *Acerca del Ministerio de Tecnologías de la Información y las Comunicaciones.* Bogotá, Colombia. Recuperado de: http://www.mintic.gov.co/portal/604/w3-propertyvalue-540.html

Organización de los Estados Americanos. (2015). *Reporte de Seguridad Cibernética e Infraestructura Crítica de las Américas.* Recuperado de: https://www.sites.oas.org/cyber/Documents/2015%20-%20OEA%20Trend%20Micro%20Reporte%20Seguridad%20Cibernetica%20y%20Porteccion%20de%20la%20Inf%20Critica.pdf

Pelcastre, J. (17 de septiembre de 2014). Ejército Nacional de Colombia protege infraestructura petrolera contra las FARC. *Dialogo Revista Militar Digital.* Recuperado de: http://dialogo-americas.com/es/articles/rmisa/features/regional_news/2014/09/17/colombia-oil-security

Pinochet, A. (1984). *Geopolítica.* 4ª ed. Chile: Editorial Andrés Bello.

Purkayastha, P. (30 de abril de 2015). ¡Haz la ciberpaz, no la ciberguerra!. América Latina en movimiento. Recuperado de: http://www.alainet.org/es/articulo/169326

Real Academia de la Lengua Española. (___). Definición de cibernética. Recuperado de: http://buscon.rae.es/drae/srv/search?val=cibern%E9tica

Redacción tecnología. (27 de abril de 2015). Aumenta ciberataques contra sistemas clave: OEA. *El Espectador.* Recuperado de:

http://www.elespectador.com/tecnologia/aumentan-ciberataques-contra-sistemas-clave-oea-articulo-557287

Redacción Tecnosfera. (24 de abril de 2015) ¿Qué tanto aporta la industria TIC a la economía nacional?. *El Tiempo.* Recuperado de: http://www.eltiempo.com/tecnosfera/novedades-tecnologia/sector-tic-crece-en-importancia-en-la-economia/15618752

Rico-Bernabé, R. (2002). *El mantenimiento de la paz ante los retos de las nuevas guerras.* Barcelona, España: Editorial Icaria.

Sánchez, M. (2012). *Protección de Infraestructuras Críticas. Un nuevo reto para la convergencia de las seguridades.* Recuperado de: http://manuelsanchez.com/2012/05/28/proteccion-de-infraestructuras-criticas-un-nuevo-reto-para-la-convergencia-de-las-seguridades/

Schiff, A. (1984) *Lifelines in an Urban Post-Earthquake Environment" in Hays, W.W., and Gori, P.L. (eds.), Proceedings of Conference XXVI-A Workshop on "Evaluation of Regional and Urban Earthquake Hazards and Risk in Utah, Salt Lake City, Utah.* Virginia, Estados Unidos: Geological Survey.

Semana. (09 de septiembre de 2014). “Hacker” Andrés Sepúlveda irá a juicio. *Revista Semana.* Recuperado de: http://www.semana.com/nacion/articulo/hacker-andres-sepulveda-ira-juicio/402190-3

Soto, V. (____). *La protección de infraestructuras críticas y el criminólogo.* Recuperado de: http://www.belt.es/expertos/HOME2_experto.asp?id=6462

Stel, E. (2014). *Seguridad y Defensa del ciberespacio.* Buenos Aires, Argentina: Editorial Dunken.