La ciberdefensa en Colombia

Villanueva Méndez Julio Cesar
julio.villanueva95@hotmail.com
Universidad Piloto de Colombia

Resumen – El ciberespacio también denominado el quinto teatro de operaciones, donde se desarrollarán las guerras del futuro, es una realidad ante la cual, Colombia no es indiferente a este nuevo escenario de guerra. Actualmente, cada Estado debe establecerse como objetivo principal definir cómo hacer frente a las amenazas que atentan contra su seguridad y la defensa en el campo cibernético. Así, Colombia en su lucha contra esta nueva amenaza cibernética decidió crear directrices a través del *Conpes 3701*; en este documento concebido para la seguridad cibernética y la política de defensa en Colombia, el gobierno dio funciones a los organismos del Estado para la creación del Grupo de Respuesta a Emergencias Cibernéticas (ColCERT), El Comando Cibernético Conjunto (CCOC) y el Comando Cibernético Policial (CCP).

Abstract – The cyberspace called the fifth operational theater, where the wars of the future will be developed and Colombia is not indifferent to this new war scenario. Currently every State should be drawn as a main goal to define how to deal with the threats that attack their security and defense in the cyber field. So Colombia in its fight against this new cyber threat decided to create guidelines through the Conpes 3701; this document created for cyber security and defense policy in Colombia, the government gave functions to State agencies for the creation of the Cybernetic Emergency Response Group (ColCERT), The Joint Cyber Command (CCOC), and the Police Cyber Command (CCP).

Índice de términos — CCOC, CCP, Ciberataque, Ciberdefensa, ColCERT, Conpes, Hacker.

I. INTRODUCCIÓN

Vivimos una época en el mundo donde nos hemos vuelto dependientes de las tecnologías de la información y las comunicaciones; cualquier sector del país sea público o privado emplea cualquier medio tecnológico para operar y desarrollarse en la sociedad, pero este mismo avance informático ha creado un reciente crecimiento en las vulnerabilidades en seguridad de la información.

Estas vulnerabilidades son aprovechadas para generar lo que definimos como ataques cibernéticos que son un método por el cual un individuo, mediante un sistema informático, intenta tomar el control, desestabilizar o dañar otro sistema informático, estos puede ser generados por diferentes tipos de actores como los mismos Estados, grupos *hacktivistas* o delincuencia que buscan un interés económico, de reconocimiento intelectual o para mejorar las ventajas militares de una nación.

Por esta razón se ha visto la necesidad de crear un nuevo teatro de operaciones como el ciberespacio y surgir una nueva disciplina como la ciberdefensa, que se centra en la fase operativa de los ciberataques y desarrollar la defensa y protección de las redes e infraestructura.

En el nuevo contexto mundial, los países, especialmente los más desarrollados han contemplado la amenaza cibernética como una de las de más alta prioridad, gracias a las características propias del ciberespacio que propician la clandestinidad, el anonimato, fácil acceso, poco o ningún control gubernamental, rápido flujo de información, indetectable, bajos costos, bajos riesgos y alto impacto por el poder en términos de la capacidad de destrucción, disrupción, mal funcionamiento o toma de control de sistemas tecnológicos y sus consecuencias, y también por la rentabilidad en términos económicos o políticos por parte de personas, industrias y Estados, constituyendo la amenaza cibernética en una

preocupación presente y futura para los Estados, más aún, cuando la dependencia tecnológica es una realidad inevitable, con la cual necesariamente tendrán que convivir los ciudadanos y la sociedad, y sobre la que se soporta cada vez más la actividad económica y social de los países. Algunas naciones ya han empezado a obtener capacidades en ciberdefensa, lastimosamente basándose en malas experiencias propias como el caso de Estonia.

II. ANTECEDENTES DE ATAQUES CIBERNÉTICOS

A. Estonia 2007

En abril de 2007, las instituciones de Estonia se vieron paralizadas por una avalancha de ciberataques. Los objetivos fueron numerosas instituciones públicas, entre ellas, el Parlamento y varios ministerios, además de bancos, partidos políticos y medios de comunicación. Estonia tuvo que cortar toda la línea de Internet y formatear todos sus sistemas.

B. El Gran Colisionador de Hadrones

El 12 de septiembre de 2008, día del estreno oficial del "acelerador de partículas", conocido como el Gran Colisionador de Hadrones (LHC), el griego grupo 'Green Security Team' consiguió hackear los sistemas informáticos del CERN de Ginebra.

C. Stuxnet

El 26 de septiembre de 2010 se descubrió que las plantas nucleares de Irán fueron atacadas por un enemigo inédito hasta la fecha en los canales de la guerra. El ataque fue perpetrado por un gusano informático, bautizado como Stuxnet, capaz de penetrar en los sistemas industriales de control que se utilizan para controlar instalaciones industriales como plantas de energía eléctrica, presas, y otros complejos industriales.

Según explican los expertos de la empresa Symantec esta amenaza estaba diseñada para permitir a los *hackers* manipular equipos físicos, una amenaza nunca antes vista. Es el primer virus informático que permite hacer daño en el mundo físico. Aunque afectó a ordenadores de todo el mundo, uno de los más afectados fue Irán. Afectó a 13 países, y 72 organizaciones acabaron afectadas.

D. Duqu.

Fue descubierto el 19 de octubre de 2011. Este *malware* es una variante del arma cibernética destinada a retrasar la capacidad de Irán para fabricar bombas nucleares, Stuxnet. Su función era reunir datos de Inteligencia y activos de entidades.

E. Flame

Fue descubierto el 28 de mayo de 2012, fue diseñado para recopilar información sensible y presente en ordenadores de Irán, Oriente Próximo e incluso Estados Unidos.

F. Gauss

El 1 de agosto de 2012 se descubrió Gauss, otro virus derivado de Stuxnet. Llegó a afectar a más de 2.500 ordenadores y concentró sus ataques en el Líbano, Israel y territorios palestinos. Su principal objetivo era recabar información de las instituciones bancarias, transacciones comerciales y otros datos.

G. China

Hasta el 5 de noviembre de 2012, China solo había podido fabricar aviones de hasta 3ª generación. Pero en esta fecha, anunció la creación del J-31, de 5ªgeneración. Esto despertó las alarmas de Estados Unidos y de Japón, ya que la estructura y la

apariencia física eran casi idénticas a aviones creados por ellos ¿Ingenio o ciberespionaje?.

H. Octubre Rojo

Investigadores rusos detectaron el 14 de enero de 2013 un ciberataque que podría haber estado robando documentos confidenciales encriptados desde 2007 de instituciones gubernamentales como embajadas y de centros de investigación nuclear y compañías estatales de gas y petróleo.

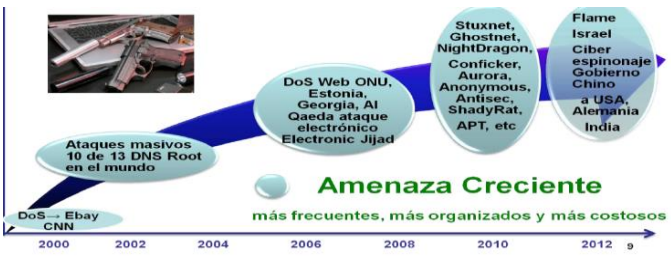
El ciberataque se basa en un *malware* diseñado para robar documentos encriptados y permite incluso sustraer documentos que han sido previamente borrados de los archivos informáticos.

I. Informe de Mandiant

La empresa Mandiant publicó un informe en el que dice que un grupo de piratas informáticos, identificados como APT-1, cuentan con el "apoyo directo del Gobierno" chino para perpetrar una "amplia campaña de espionaje cibernético a largo plazo".

Mandiant ha localizado el origen de ataques a 141 entidades de todo el mundo -la mayoría de ellas de países angloparlantes- a las puertas de un edificio en las afueras de Shanghai, donde opera la unidad 61398 del Ejército de Liberación Popular chino.

Gráfica 1. Antecedentes de ataques cibernéticos



Escuela Superior de Guerra. (2014). Ciberseguridad y ciberdefensa.

III. COLOMBIA Y EL CONPES 3701

Gráfica 2. Países latinoamericanos más afectados por una red de zombies.

No.	PAÍS	%
1	INDIA	19.14
2	MÉXICO	12.85
3	BRASIL	7.74
4	COREA	7.24
5	COLOMBIA	4.94
6	RUSIA	3.14
7	EGIPTO	2.99
8	MALASIA	2.86
9	UCRANIA	2.69
10	PAKISTAN	2.55

No.	PAÍS	%
11	PERÚ	2.42
12	IRÁN	2.07
13	ARABIA SAUDÍ	1.85
14	CHILE	1.74
15	KAZAKHSTAN	1.38
16	EMIRATOS ARABES	1.15
17	MARRUECOS	1.13
18	ARGENTINA	1.10
19	ESTADOS UNIDOS	1.05

Recuperado de: http:// infospyware.com /red de zombies en marzo 2010.

En este tema de Colombia no es un país ajeno a los ataques cibernéticos y es uno de los países latinoamericanos con más ataques e infecciones a sus redes informáticas, y podemos referenciarlos con el *hackeo* a la cuenta de correo del presidente Juan Manuel Santos la máxima autoridad del país quien es la persona más custodiada en términos de seguridad del país, pero que en temas de seguridad informática demostró que ni el mismo presidente está seguro y es vulnerable.

Gráfica 3. Hackeo página presidente de Colombia

Recuperado de: http://geektheplanet.net/5642/juan-manuel-santos-se-une-a-anonymous.xhtml.

Por este motivo en el año 2011 se realizó el Consejo Nacional de Política Económica y Social, *Conpes 3701* donde se crearon los lineamientos de política para ciberseguridad y ciberdefensa en Colombia.

Se buscaba desarrollar una estrategia nacional que contrarrestara el incremento de las amenazas informáticas que afectan significativamente al país. Adicionalmente, recoger los antecedentes nacionales e internacionales, así como la normatividad del país en torno al tema.

El *Conpes 3701* identificó tres temas esenciales para poder iniciar los lineamientos de ciberdefensa en el país los cuales son:

1. Las iniciativas y operaciones en ciberseguridad y ciberdefensa no están coordinadas adecuadamente.

A pesar de existir algunos esfuerzos institucionales (tanto privados como públicos), se ha identificado que no existen organismos a nivel nacional constituidos para coordinar y desarrollar operaciones de ciberseguridad y ciberdefensa.

Por tanto, no ha sido posible implementar los mecanismos suficientes y adecuados para contrarrestar ataques cibernéticos y proteger los intereses del Estado en el ciberespacio. Se evidencia una debilidad en la difusión, concienciación, generación de una cultura de prevención y acción segura en ciberseguridad, dirigida tanto al sector público como al privado, así como a la sociedad civil.

2. Debilidad en la oferta y cobertura de capacitación especializada en ciberseguridad y ciberdefensa.

El conocimiento en el área de ciberseguridad y ciberdefensa tanto en el sector público como en el privado es limitado. Si bien en el país existen algunas instituciones de educación superior que ofrecen especializaciones en seguridad informática y derecho informático, se ha identificado que la oferta académica en programas especializados en estas áreas es reducida. En consecuencia, un número significativo de personas que acceden a algún tipo de formación en el área de seguridad de la información, lo hacen mediante programas ofrecidos por instituciones extranjeras, en los que no se profundiza sobre la realidad colombiana.

3. Debilidad en regulación y legislación de la protección de la información y de los datos.

Pese a que existen instrumentos legales y regulatorios en seguridad de la información, persisten falencias que impiden responder oportunamente a incidentes y delitos cibernéticos.

En cuanto a normatividad internacional, dentro de los instrumentos que le permitirían al país integrarse a la comunidad mundial está la Convención del Consejo de Europa en Delito Cibernético, que requiere cumplir con aspectos como el establecimiento de mecanismos de cooperación judicial como la extradición, la creación de puntos de contacto localizables las 24 horas del día los 7 días a la semana para facilitar la investigación y el mantenimiento de los *logs* por parte de los ISPs, durante el tiempo necesario.

4. Objetivo Central

Fortalecer las capacidades del Estado para enfrentar las amenazas que atentan contra su seguridad y defensa en el ámbito cibernético (ciberseguridad y ciberdefensa), creando el ambiente y las condiciones necesarias para brindar protección en el ciberespacio.

Para este fin es necesario involucrar a todos los sectores e instituciones del Estado con responsabilidad en el campo de ciberseguridad y ciberdefensa, creando un ambiente participativo donde todos los actores de la sociedad actúen con propósitos comunes, estrategias concertadas y esfuerzos coordinados. Igualmente, es de vital importancia crear conciencia y sensibilizar a la población en todo lo referente a la seguridad de la información; fortalecer los niveles de cooperación y colaboración internacional en aspectos de ciberseguridad y ciberdefensa; apoyar investigaciones relacionadas con ataques

informáticos y proteger a la ciudadanía de las consecuencias de estos ataques.

Analizando esta problemática el *Conpes 3701* implementó un objetivo central el cual fue implementar instancias apropiadas para prevenir, coordinar, atender, controlar, generar recomendaciones y regular los incidentes o emergencias cibernéticas para afrontar las amenazas y los riesgos que atentan contra la ciberseguridad y ciberdefensa nacional, los cuales quedaron definidos de la siguiente manera:

a. Una Comisión Intersectorial encargada de fijar la visión estratégica de la gestión de la información. Esta Comisión estaría encabezada por el Presidente de la República e integrada como mínimo por el Alto Asesor para la Seguridad Nacional, el Ministro de Defensa Nacional, el Ministro de Tecnologías de Información y Comunicaciones, el Director del Departamento Administrativo de Seguridad – DAS o quien haga sus veces, el Director de Planeación Nacional y el Coordinador del ColCERT.

b. El Grupo de Respuesta a Emergencias Cibernéticas de Colombia – ColCERT 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.

Gráfica 4. Instituciones creadas por el Conpes 3701

Comando Conjunto Cibernético. (2013). Fuerzas Militares de Colombia y el Conpes 3701.

Estas instituciones al depender del Ministerio de Defensa Nacional, son sabedoras del alcance de su responsabilidad al encarar los desafíos que la revolución de las tecnologías de la información, cifran como una realidad donde el ciberespacio es el quinto dominio en el cual las personas pueden interactuar en armonía, cooperación y/o conflicto.

Las Fuerzas Militares de Colombia, tratarán el ciberespacio como un ámbito estratégico, operativo y táctico, para organizar, entrenar y equipar a fin de aplicar medidas de prevención, disuasión, contención, protección y reacción, que permita fortalecer las capacidades de Ciberdefensa, para enfrentar las amenazas o incidente informáticos que puedan afectar la infraestructura crítica del país y poner en riesgo la Seguridad Nacional, la defensa de la soberanía y el orden constitucional del Estado así como causar daños masivos, debilitar la economía, y/o dañar la moral pública y la confianza.

Por esto, el trabajo al interior de las Fuerzas Militares, concentra en el Comando Conjunto Cibernético la coordinación con las Unidades Cibernéticas del Ejército Nacional, la Armada Nacional y la Fuerza Aérea Colombiana.

Cada una de estas Unidades Cibernéticas es responsable de realizar la Ciberseguridad de su propia Fuerza y la Ciberdefensa de las Infraestructuras Críticas Propias y las que le sean asignadas bajo su responsabilidad de acuerdo con su rol misional.

IV. ESTRATEGIA DE LA CIBERDEFENSA DEL ESTADO COLOMBIANO

La Estrategia de Ciberdefensa se caracteriza por seis componentes principales en los que las Fuerzas Militares de Colombia han soportado el desarrollo de capacidades de Ciberdefensa y su fortalecimiento, así:

- Personas

La Selección del personal que trabaja en Ciberdefensa es un proceso por competencias soportado en un plan de carrera para los oficiales y suboficiales.

Capacitación y entrenamiento continúo tanto a nivel nacional como internacional.

Garantizar la baja rotación del personal a fin de evitar las inversiones de capacitación.

- Procesos

Estandarización de procesos en la parte ciber y de gestión de incidentes.

Aplicación de normas y estándares internacionales.

- Tecnología:

La adquisición de tecnología es planeada desde varios puntos de vista como son:

- Funcionamiento y servicios.
- Operaciones de Ciberdefensa.
- Investigación+Innovación+Desarrollo.
- Laboratorios para investigación.
- Observatorios.

- Cooperación

Es uno de los componentes fundamentales. Se hace a nivel nacional e internacional en los Sectores Públicos, Privados, Academia, Ciudadanía y Fuerzas Armadas.

- Operaciones

Se hizo necesario desarrollar una estrategia Militar de Ciberdefensa, doctrina.

- Fundamento Legal

A pesar de no ser los directos responsables de la doctrina, se ha buscado socializar en diferentes escenarios sobre la necesidad de fortalecer las normas y leyes a nivel nacional.

Recomendaciones expertos Internacionales

- Fortalecimiento de las capacidades Institucionales de Ciberseguridad y Ciberdefensa.
- Política para la protección de infraestructura crítica.
- Crear un órgano de coordinación permanente.
- Establecimiento y mejora de los marcos legales en Ciberseguridad.
- Generación de Capacidades de Ciberdefensa.
- Capacidad analítica y técnica - tendencias de la amenaza.
- Academia de Cibernética Profesional.
- Establecer Centros de Innovación /Excelencia.
- Cooperación Internacional y Cooperación entre múltiples partes interesadas.
- Estrategia para la cooperación internacional.
- Ampliar el papel del Ministerio de Relaciones Ext.
- Coordinador de Política Cibernética Internacional.
- Invertir en un plan de capacitación internacional.
- Establecer cooperación entre el sector público y privado, nacional e internacional.

Línea de tiempo construcción de la Ciberdefensa para el país

Gráfica 5. Línea de tiempo

Comando Conjunto Cibernético. (2014). Ciberdefensa y Ciberseguridad 2014-2018.

V. RETOS E INICIATIVAS EN CIBERDEFENSA

- COLCERT
- Implementación del equipo de emergencias cibernéticas ColCERT.
- Respuesta en línea a incidentes de Ciberseguridad ColCERT.
- Convenio con dominio .CO
- Base de datos contactos nacionales / Internacionales.

- CCOC
- Implementación del Comando Conjunto Cibernético.
- Respuesta en línea a incidentes de Ciberseguridad SOC.
- Definición de sectores estratégicos.
- Desarrollo de Capacidades avances en doctrina militar ciber.
- Implementación de las Unidades de Ciberdefensa en las diferentes Fuerzas Militares.

- CCP
- Implementación del Centro Cibernético Policial C.C.P.
- Respuesta en línea a incidentes de Ciberseguridad Cuadrante Virtual - CAI VIRTUAL.
- Coordinación Internacional Interpol Europol Grupo de Trabajo de Delitos Tecnológicos.
- Atención de incidentes informáticos DIJIN Laboratorios móviles de informática forense.
- Implementación CSIRT PONAL (Equipo de Respuesta a Incidentes Informáticos de la Policía Nacional).

VI. INFRAESTRUCTURA CRÍTICA DIGITAL DEL PAÍS

Como uno de los proyectos más importantes que se generaron gracias al *Conpes 3701* fue darle importancia a la seguridad de la infraestructura critica digital del país, donde en cabeza del Comando Conjunto Cibernético y con la colaboración de más de 10 Ministerios y varias empresas de diferentes sectores, se dio la tarea de identificar la infraestructura crítica y desarrollar medidas para enfocar recursos y articular esfuerzos para su protección y fortalecimiento.

Igualmente, orientados a tornar a Colombia en un Estado cibernéticamente seguro y blindado de cualquier amenaza, este trabajo iniciado en diciembre de 2013, hasta la fecha concluye que gracias a su esfuerzo ya se identificaron 17 Sectores que impactan desde el componente económico, político y/o social a Colombia.

Y como todos los sectores del desarrollo económico y social están comprometidos con este cometido, las fases para su consolidación y desarrollo aportarán al país, una gran lección aprendida en materia de seguridad tecnológica a la vanguardia de lo que el escenario mundial exige, en aras igualmente, del fortalecimiento de la ciberdefensa de la FF.MM.

Gráfica 6. Comité de infraestructura crítica del país

Comando Conjunto Cibernético. (2015). Infraestructura crítica digital.

VII. CONCLUSIÓN

Se identifica que la Ciberdefensa es una realidad emergente que deben considerar las naciones como un elemento estratégico de gobernabilidad en el siglo XXI.

También definir que el ciberespacio es el quinto dominio de la guerra y el Estado debe trazar como objetivo central, examinar el fortalecimiento de sus capacidades para enfrentar las amenazas que atentan contra su seguridad y defensa en el ámbito cibernético, y para ello debe identificar tres tareas específicas sobre las cuales cimentar la ruta de análisis.

En primer término, implementar instancias apropiadas para prevenir, atender, controlar y generar recomendaciones que regulen los incidentes y/o emergencias cibernéticas para proteger la infraestructura crítica nacional; en segundo lugar, diseñar y ejecutar planes de capacitación especializada en ciberseguridad y ciberdefensa y como tercer fin, fortalecer el cuerpo normativo y de cumplimiento en la materia con miras a desarrollar las herramientas jurídicas necesarias para una efectiva y eficiente prevención, investigación y judicialización de los delitos cibernéticos.

Gráfica 7. Países a la vanguardia de la ciberdefensa

Comando Conjunto Cibernético. (2014). Ciberdefensa y Ciberseguridad.

BIBLIOGRAFÍA

Fuentes académicas

Betz, David J. & Stevens, Tim (2013). Cyberspace and the state.

Libicki, Martin (2012). Cyberdeterrence and Cyberwar. U.S.A.: RAND project Air Force.

Fuentes institucionales

Documento Conpes 3701, Lineamientos de política para ciberseguridad y ciberdefensa (2011).

Fuentes electrónicas

[www.teinteresa.es] (19 abril 2013) en línea consultado el 26, 07-15.

[www.Infospyware] (marzo 2010) en línea consultado el 26, 07-15.