PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

FACULTAD DE CIENCIAS HUMANAS

ESCUELA DE SOCIOLOGÍA CON MENCIÓN EN RELACIONES INTERNACIONALES

DISERTACIÓN PREVIA A LA OBTENCIÓN DEL TÍTULO DE

SOCIÓLOGA CON MENCIÓN EN RELACIONES INTERNACIONALES

DESAFÍOS DE LA CIBERSEGURIDAD Y RESPUESTAS ESTATALES: EL CASO DEL ESTADO ECUATORIANO EN EL PERÍODO 2008 - 2015.

FRANCIS STEPHANÍA MOGOLLÓN FLORES

DIRECTOR: ECON. MARCO ROMERO CEVALLOS

QUITO, 2017

DEDICATORIA

Este trabajo lo dedico especialmente a Dios, a mis padres Edison Mogollón y Carmen Flores, a mi hermano Edison Mogollón, a mi cuñada Evelin Espinosa y a los dos amores de mi vida Maximiliano Mogollón y José Luís Jiménez.

AGRADECIMIENTO

A Dios por darme la fuerza y la convicción para culminar una etapa más en mi vida, por bendecirme cada día y acompañarme en cada paso de mi carrera.

A mis padres por haberme apoyado en todo momento, gracias a su amor incondicional y sus palabras oportunas he alcanzado esta meta con éxito.

A mi hermano que ha sido mi modelo a seguir, alguien que jamás me deja sola y que me impulsa hacia adelante.

A mi Maximiliano que es mi razón de ser, la personita por la que me levanto todos los días con una sonrisa y que me motiva para ser cada día mejor.

A José Luís Jiménez por ayudarme a seguir adelante, por su amor y dedicación, por hacerme saber que soy capaz y estar a mi lado en todo este proceso.

A mis profesores, que me impartieron valores y conocimientos para desarrollarme personal y profesionalmente.

A mi director de tesis, Econ. Marco Romero Cevallos, que me brindó su conocimiento, apoyo y paciencia para culminar este trabajo.

TABLA DE CONTENIDO

RESUMEN

La ciberdefensa se ha vuelto un aspecto fundamental para la seguridad nacional de cualquier país dado que las guerras ahora se están desarrollando en un nuevo campo que es el ciberespacio. Esto ha generado nuevas amenazas para la seguridad nacional, amenazas de las cuales nadie está exento. Estas nuevas amenazas han hecho no solo que los Estados asignen a diferentes instituciones la responsabilidad de estructurar una ciberseguridad óptima para garantizar su supervivencia, sino también que busquen soluciones multilaterales.

El Ecuador como país en vías de desarrollo presenta diversas vulnerabilidades frente a las ciberamenazas, de modo que el presente trabajo de titulación previo a la obtención del título de Sociología con mención en Relaciones Internacionales, se centrará en develar los desafíos de la ciberseguridad y las respuestas estatales que ha llevado a cabo el Estado ecuatoriano en el período 2008 -2015.

Esta investigación mostrará el desarrollo de las amenazas cibernéticas a nivel global, para posteriormente determinar cuáles han sido las respuestas individuales y multilaterales de los países más relevantes en materia de ciberseguridad, frente a las ciberamenazas. También se analizará el contexto regional y las respuestas multilaterales que han llevado a cabo los países sudamericanos.

Finalmente aterrizaremos en el caso ecuatoriano y estudiaremos la estrategia de ciberseguridad que maneja el país, en base al análisis de las instituciones encargadas de velar por su seguridad cibernética, la legislación del Estado en materia de ciberseguridad y sus respuestas, para así poder alcanzas el fin último de este trabajo.

INTRODUCCIÓN

Planteamiento del Problema

El uso masivo de las Tecnologías de la Información y Comunicación (TIC) ha tenido efectos trascendentales en lo político, lo social y lo económico de todos los países. Esta globalización tecnológica ha traído consigo aspectos positivos como por ejemplo la generalización del conocimiento, nuevos medios de producción y ha permitido el acceso por parte de sus usuarios a un abanico de servicios (García L. F., 2013). Pero estos adelantos tecnológicos no solo están siendo utilizados para el bien de la humanidad, sino que también se usan para los intereses ilícitos de algunos individuos, grupos o Estados.

> *"*Gran parte de la vida moderna depende de las computadoras y las redes informáticas. Para muchas personas, la interacción más visible que tienen con las computadoras es escribir en el teclado. Pero las computadoras y las redes son críticas para funciones clave como la gestión y operación de centrales nucleares, represas, la red de energía eléctrica, el sistema de control de tráfico aéreo y la infraestructura financiera. Las computadoras también son fundamentales en las operaciones diarias de las empresas, las organizaciones y el gobierno. Las empresas grandes y pequeñas dependen de computadoras para administrar la nómina, realizar un seguimiento de inventario y ventas, y realizar investigación y desarrollo. La distribución de alimentos y energía desde el productor hasta el consumidor minorista depende de ordenadores y redes en cada etapa." (Computer Science and Telecommunications Board, Division on Engineering and Physical Sciences and National Research Council of EEUU, 2002, pág. 2)

Debido a que las TICs se han vuelto parte de nuestro día a día, la sociedad, las empresas, los Estados y la defensa nacional dependen del funcionamiento de estas tecnologías, y de la operación de Infraestructuras Críticas de la

Información[1]. Todo esto nos deja ver como la sociedad moderna y los países desarrollados y en vías de desarrollo son cada vez más dependientes de los sistemas informáticos, con lo cual son más vulnerables ante las ciberamenazas[2]. Las sociedades interconectadas van en aumento y, a pesar de los riesgos que corren, es una tendencia que no se va a detener, lo que nos indica que hay que gestionar los riesgos que se presentarán a futuro.

En la actualidad se aprecia que los delitos cibernéticos se han vuelto mucho más sofisticados, se han complejizado las actividades de ciberespionaje militar, industrial y político, y se han incrementado los ciberataques a estructuras críticas, tanto por parte de grupos organizados como por individuos (los individuos pueden actuar por ignorancia, diversión, curiosidad, reto intelectual o lucro). Esto se debe a que el ciberespacio es muy atractivo por ser un ambiente complejo y anárquico, que ofrece una anonimización[3] casi total a los autores de los ataques. En el ciberespacio también existe una desproporción entre los esfuerzos que se requieren para la protección de los sistemas y los pocos medios que necesita el ciberagresor para materializar una amenaza.

Los ciberataques a Estructuras Criticas o a Sistemas Informáticos pueden tener graves repercusiones en la sociedad y su economía, es decir pueden afectar a todos los niveles de la sociedad. Esto nos permite ver cómo es que, a medida que las sociedades dependen más de las TICs, la ciberseguridad se ha vuelto uno de los retos más importantes del siglo y un tópico de interés nacional (Leiva, 2015, pág. 161).

[1] "El transporte, las comunicaciones, el comercio electrónico, los servicios financieros, los servicios de emergencia y servicios públicos se sustentan en la disponibilidad, integridad y confidencialidad de la información que fluye a través de estas infraestructuras." (Leiva, 2015, pág. 163)

[2] "Actividades realizadas en el ciberespacio, que tienen por objeto la utilización de la información que circula por el mismo, para cometer distintos delitos mediante su utilización, manipulación, control o sustracción." (Días, 2016, pág. 3)

[3] Los ciberataques se llevan a cabo de una forma anónima de modo que sea casi imposible detectar a su autor, y en caso de que se lo detecte este ya haya cumplido su cometido. Se busca actuar anónimamente en línea para realizar transacciones financieras fraudulentas o lanzar ataques con poco riesgo de ser localizados por las agencias policiales y con el objetivo evitar las consecuencias de un comportamiento criminal o socialmente inaceptable. (Weber & Heinrich, 2012, pág. 5)

En base al riesgo que representa el mal uso del ciberespacio y de las TICs para la democracia y el bienestar de un país, surge la necesidad de utilizar herramientas para la prevención y defensa ante ataques cibernéticos. Se hace necesario plantear una Estrategia Nacional de Ciberseguridad[4] para garantizar la supervivencia de la nación; un plan que defienda sus legítimos intereses, y mejore la seguridad tanto de las estructuras críticas como de los sistemas informáticos nacionales.

Mohammed Ayoob analiza el predicamento de seguridad que viven los países del tercer mundo, que al no tener estabilidad, deben preocuparse tanto de las amenazas externas a su seguridad como de la supervivencia propia. Este predicamento tienen tres elementos clave, los cuales son: la falta de legitimidad del Estado, instituciones estatales y regímenes; la falta de cohesión social; y la falta de consenso nacional (Medina, 2007, pág. 23). Esta problemática se traduce a la ciberseguridad ya que la falta de legitimidad de los Estados, instituciones y regímenes de los países de tercer mundo hace que su seguridad cibernética no sea integral y efectiva.

Con esto Ayoob no quiere decir que los países desarrollados hayan alcanzado una ciberseguridad integral y optima, pero plantea una diferencia crucial en cuanto al tiempo, los Estados de los países de primer mundo tienen mucho más tiempo de creación y por ende han podido solventar algunos de los problemas que presenta la seguridad nacional, lo que no sucede en los países del llamado tercer mundo.

El Ecuador como país periférico y en vías de desarrollo presenta diversas vulnerabilidades ante las amenazas cibernéticas que examinaremos más adelante; es necesario por lo tanto , preguntarse cómo optimizar los limitados recursos económicos, humanos, teóricos y financieros disponibles en este campo,

[4] "desarrollo de capacidades y habilidades en la prevención, defensa, detección, análisis, investigación, recuperación y respuesta a las amenazas, como así también la gestión de los riesgos asociados." (Leiva, 2015, págs. 161-162)

y cómo construir estructuras bien definidas que permitan garantizar la protección de la información sensible que maneja el Estado; así como la privacidad y confidencialidad de sus ciudadanos, organizaciones y sistemas.

La dependencia de TICs extrajeras representa un riesgo para la ciberseguridad del Ecuador, ya que el software no le permite al usuario realizar modificaciones libremente de modo que no puede solventar las falencias de seguridad del sistema. Cada actualización o cambio que se quiera hacer en el programa debe ser autorizado por su creador y en muchos de los casos, cuando los cambios son aprobados, hay que pagar altas sumas de dinero para llevarlos a cabo, caso contrario se debe esperar a que el proveedor del software realice la actualización, la cual también requieren de un pago. Es decir que el software extranjero no permite que las empresas públicas y privadas que lo utilizan, gestionen libremente los aspectos de seguridad del mismo.

El hecho de que el Ecuador sea un país periférico supone, desde el enfoque de Mohammed Ayoob, un déficit de estatalidad que también lo vuelve más vulnerable frente a las ciberamenazas, pues “la falta de estatalidad hace que los Estados sean extremadamente vulnerables a las presiones externas – políticas, militares, económicas o tecnológicas – de otros Estados usualmente más desarrollados, de instituciones internacionales, y de actores transnacionales” (Medina, 2007, pág. 16).

Pregunta de Investigación

¿Cuál es la situación del Estado Ecuatoriano ante las ciberamenazas durante el periodo 2008 - 2015?

La pregunta se ha formulado debido a que el Ecuador, como todos los demás países, al estar articulado a varias redes globales dentro de las cuales se maneja información sensible , principalmente secretos industriales e información financiera, económica y política, es vulnerable y debe mejorar el manejo de su

ciberseguridad. Para responder a la pregunta de investigación en primera instancia analizaremos el contexto global y regional de la ciberseguridad para posteriormente aterrizar en el caso ecuatoriano, dentro del cual observaremos los antecedentes fundamentales de las ciberamenazas que enfrenta el Ecuador, las respuestas individuales y multilaterales que ha llevado a cabo el Estado, las capacidades de las entidades públicas llamadas a velar por la ciberseguridad del país y la legislación definida en materia de ciberseguridad.

Marco Conceptual

Previo a exponer el enfoque teórico de este trabajo investigación, es preciso presentar los conceptos fundamentales que serán utilizados a lo largo de su desarrollo. Primeramente expondremos la concepción de Estado de Francisco Porrús Perez, seguido del concepto de ciberseguridad de Bayuk, Healey, Rohmeyer, Sachs, Smitdt y Weiss y finalmente describiremos la noción del complejo de seguridad que presenta Buzan, Waever y de Wilde.

Estado

Para propósito de este trabajo voy tomar dos concepciones de Estado de Francisco Porrúa Pérez, que señala lo siguiente:

> "El estado es una sociedad humana establecida en el territorio que le corresponde, estructurada y regida por un orden jurídico, que es creado, definido y aplicado por un poder soberano, para obtener el bien público temporal, formando una institución con personalidad moral y jurídica." (Pérez F. P., 2005, pág. 27)

> "El Estado como ente cultural tiene por objeto la obtención de un fin. Ya sabemos que todo producto de la cultura se caracteriza por llevar dentro de sí una finalidad, aquello para lo cual es creado por el hombre. Siendo el Estado una institución humana, tiene naturalmente un fin. No

> puede dejar de tenerlo. Los hombres que componen el Estado, los gobernantes y los gobernados, al agruparse formando la sociedad Estatal persiguen un fin. El Estado encierra en su actividad una intención que es la determinante y el motor de toda su estructura… El fin será el que determine las atribuciones, la competencia material de los diferentes órganos del Estado, y en función de esa competencia se crearán órganos. En este fin está la razón última del Estado y su diferencia especifica con otras sociedades" (Pérez F. P., 2005, pág. 284)

De acuerdo con esta perspectiva, determinaremos el objetivo de la ciberseguridad, las atribuciones del Estado ecuatoriano y sus competencias materiales para crear nuevos órganos, normas y políticas que contribuyan a este fin.

Seguridad

Tomaremos los postulados de Kenneth Waltz, Barry Buzan, Lene Hansen y Ole Waever:

Barry Buzan y Lene Hansen, para analizar el concepto de seguridad, nos sugieren *"ver a la "seguridad" apoyada o conducida a través de tres tipos de conceptos: primero, a través de conceptos complementarios, como "estrategia", "disuasión", "contención" o "humanitarismo"….En segundo lugar, a través de conceptos paralelos, como "poder", "soberanía" o "identidad" ; y en tercer lugar, los conceptos de oposición que trabajan a través de la seguridad, la "paz" y el "riesgo"."* (Buzan & Hansen, 2009, pág. 14)

Esta perspectiva de seguridad va a ser sumamente útil para analizar la ciberseguridad, ya que dentro del ciberespacio vemos que todos los elementos antes mencionados existen y pueden ser utilizados.

Para Ole Waever, desde la concepción tradicional político-militar, "la seguridad se trata de la supervivencia. Es cuando un problema se presenta como una amenaza existencial hacia un objeto referente designado (tradicionalmente, pero no necesariamente, al Estado, incorporando gobierno, territorio y sociedad). El carácter especial de las amenazas a la seguridad justifica el uso de medidas extraordinarias para hacerlas efectivas. La invocación de la seguridad ha sido la clave para legitimar el uso de la fuerza, pero más generosamente ha abierto el camino para que el Estado movilice o tome poderes especiales para manejar amenazas existentes. Tradicionalmente, al decir "seguridad", un representante estatal declara una condición de emergencia, reclamando así el derecho a usar cualquier medio que sea necesario para bloquear el desarrollo de una amenaza." (Buzan, Waever, & de Wilde, 1998, pág. 21)

El postulado antes mencionado se complementa con la tesis de Kenneth Waltz que nos plantea, desde el neo-realismo, "que los Estados sirven a sus propios intereses en el sistema internacional siguiendo un estricto código de autoayuda debido a la ausencia de autoridad sobre ellos. Además, como todos los Estados existen en un estado de anarquía en el ámbito internacional de la política, todos persiguen el interés propio y tratan de adquirir poder para asegurarse y asegurar su supervivencia en un sistema donde ningún otro Estado o autoridad vendrá a salvarlos si no lo hacen." (Jehangir, 2012)

Las concepciones de Waever y Waltz son coherentes con el tema de investigación planteado, ya que el ciberespacio es un ambiente anárquico donde cada país tiene que buscar su supervivencia y utilizar los mecanismos necesarios para evitar que una amenaza cibernética se desarrolle, lo cual legitima incluso el uso de ciberataques.

Ciberseguridad

La ciberseguridad se ha tornado en una prioridad, como lo veremos a lo largo de la investigación, para la seguridad nacional de todos los Estados,

pues es clave para su supervivencia. Para entender mejor este concepto y su importancia me apoyo en la concepción de varios autores, que entienden a la ciberseguridad como "la capacidad de controlar el acceso a los sistemas en red y a la información que contienen. Donde los controles de ciberseguridad son efectivos, el ciberespacio se considera una infraestructura digital fiable, resistente y confiable. Cuando los controles de seguridad cibernética están ausentes, incompletos o mal diseñados, el ciberespacio se considera el salvaje oeste de la era digital. Incluso aquellos que trabajan en la profesión de seguridad tendrán una visión diferente de la seguridad cibernética en función de los aspectos del ciberespacio con los que interactúan personalmente. Ya sea que un sistema sea una instalación física o una colección de componentes del ciberespacio, el papel de un profesional de seguridad asignado a ese sistema es planificar ataques potenciales y prepararse para sus consecuencias." (Bayuk, Healey, Rohmeyer, Sachs, Smitdt y Weiss, 2012, pág. 1)

Es decir que, como lo estipula el Consejo de Ciencias de Computación y Telecomunicaciones, la División de Ingeniería y Ciencias Físicas y el Consejo Nacional de Investigación de los Estados Unidos, la "seguridad se refiere a la protección contra la divulgación no deseada, modificación o destrucción de datos en un sistema y también a la salvaguardia de los propios sistemas. La seguridad y la confiabilidad juntas nos garantizan que el sistema hará lo que se espera que haga." (Computer Science and Telecommunications Board, Division on Engineering and Physical Sciences and National Research Council of EEUU, 2002, pág. 19)

Complejo de Seguridad

Tomando como referente a Barry Buzan, Ole Waever y Jaap de Wilde, vemos que "el complejo de seguridad se define como un conjunto de Estados cuyas principales percepciones y preocupaciones de seguridad están tan interrelacionadas que sus problemas de seguridad nacional no

pueden analizarse o resolverse de forma razonable sin tomar en cuenta la seguridad del otro. La dinámica formativa y la estructura de un complejo de seguridad son generadas por los Estados dentro de ese complejo, por sus percepciones de seguridad e interacciones mutuas." (Buzan, Waever, & de Wilde, 1998, pág. 23) Es decir que un país no puede hablar de ciberseguridad sin generar inseguridad en el otro, lo que complejiza el desarrollo de una seguridad integral.

Marco Teórico

Para propósito de la investigación analizaremos principalmente los enfoques teóricos de Waever que se basan en la supervivencia del Estado, de Buzan y de Wilde acerca de la seguridad del Estado y la securitización, y de Bayuk, Healey, Rohmeyer, Sachs, Schmidt y Weiss sobre la ciberseguridad. También veremos los debates que se han generado en torno a las ciberseguridad según Halpin, Trevorrow, Webb, Wright, Parks y Francisco Pérez. Esto se desarrollara más ampliamente en el capítulo 1.

La seguridad internacional, como nos dice Waever, se centra en la supervivencia del Estado. Cuando los problemas externos de un país representan una amenaza existencial al Estado, este puede utilizar las herramientas y medidas que le parezcan pertinentes para evitar ser afectado.

Buzan, Waever y de Wilde analizan a la seguridad desde 5 sectores clave para la conservación del Estado: "La seguridad militar que se refiere a los dos niveles de interacción de la ofensiva armada y las capacidades defensivas de los Estados, y la percepción acerca de las intenciones del otro. La seguridad política que contempla la estabilidad organizativa de los Estados, sistemas de gobierno y las ideologías que les dan legitimidad. La seguridad económica que se basa en el acceso a los recursos, finanzas y mercados para mantener niveles aceptables de bienestar y poder estatal. La seguridad social que se refiere a la sostenibilidad, dentro de condiciones aceptables para la evolución de los patrones de lenguaje,

costumbre y de la identidad nacional. Y la seguridad medioambiental que ve al mantenimiento de la biosfera local y planetaria como el sistema de apoyo esencial del que dependen todas las demás empresas humanas." (Buzan, Waever, & de Wilde, Security, A New Framework for Analysis, 1998, pág. 8)

Debido a que la tecnología ahora forma parte de nuestra vida cotidiana, todos los sectores de seguridad antes mencionados presentan varios procesos y dinámicas que se han trasladado al ciberespacio, es decir que el ciberespacio se ha securitizado[5]. Buzan, Waever y de Wilde exponen dos niveles de actores securitizantes: a nivel del sistema internacional que en este caso sería la ONU; y, a nivel nacional, que sería el gobierno ecuatoriano. La securitización del ciberespacio nos permite hablar en la actualidad de la ciberseguridad.

Tanto la seguridad física como la seguridad cibernética tienen como objetivo prevenir, detectar y responder ante ataques rivales. El primer objetivo de ambas seguridades es prevenir un ataque; sin embargo no es posible tomar esta acción contra todo tipo de ataques, por lo que la seguridad se debe apoyar en el segundo objetivo mediante métodos de detección de ataques en curso, de ser posible antes de que ocasionen daño. El tercer objetivo se cumple cuando se evidencia que un sistema es amenazado, aun cuando no se haya detectado una amenaza en curso, es decir que si se sabe que un sistema está en riesgo, la seguridad de un Estado está facultada para responder ante este incidente. "La respuesta típicamente incluye repeler el ataque, tratar a los supervivientes humanos y salvaguardar los bienes dañados." (Bayuk, et al, 2012, pág. 2)

Según Bayuk, Healey, Rohmeyer, Sachs, Schmidt y Weiss, la ciberseguridad pone especial énfasis en salvaguardar los bienes dañados, de modo que la planificación de la seguridad debe contemplar una gestión para la completa reconstrucción y recuperación de los sistemas críticos. Esto se debe a que las

[5] "Si mediante un argumento sobre la prioridad y la urgencia de una amenaza existencial el agente securitizador ha logrado liberarse de los procedimientos o reglas que de otro modo estaría obligado, estamos siendo testigos de un caso de securitización." Barry Buzan citado en (Buzan & Hansen, The Evolution of International Security Studies, 2009, pág. 214)

tecnologías de información brindan facilidades para reconstruir los datos y programas necesarios para operar los sistemas, y solucionar completamente el problema, lo cual supone una carta abierta para que la ciberseguridad pueda mejorar continuamente. (Bayuk, et al, 2012, pág. 2)

El Consejo de Ciencias de Computación y Telecomunicaciones, la División de Ingeniería y Ciencias Físicas y el Consejo Nacional de Investigación de los Estados Unidos, en su texto "Cybersecurity TODAY and TOMORROW", está de acuerdo con lo anteriormente expresado sobre la ciberseguridad y lo complementan diciendo que los mecanismos, procedimientos y normas que se apliquen deben estar apoyadas en la política para ser eficaces, de lo contrario no existiría un órgano legal que pueda sancionar la violación a la seguridad de un sistema crítico. "Para ser útil, una política de seguridad no sólo debe indicar la necesidad de seguridad sino también abordar la gama de circunstancias bajo las cuales esa necesidad debe ser cumplida y las normas operativas asociadas." (Computer Science and Telecommunications Board, Division on Engineering and Physical Sciences and National Research Council of EEUU, 2002, pág. 19)

La ciberseguridad representa un dilema de seguridad, puesto que si el ciberespacio es una zona anárquica, cada Estado busca su supervivencia, y esto lo faculta a usar los mecanismos necesarios para mantener su ciberseguridad. Como señala Barry Buzan, ningún país se puede asegurar dentro del ciberespacio, sin causar inseguridad a otros. Sin embargo no solo los Estados enfrentan este dilema de seguridad, es por ello que dentro de la investigación, nos vamos a basar en el "Dilema de Seguridad Heterogéneo", ya que toma en cuenta a otros actores presentes en el ciberespacio, como por ejemplo: individuos, bandas terroristas, grupos delictivos y empresas (Medina, 2007, pág. 21).

Los debates que se han dado entorno a la ciberseguridad han sido los siguientes:

- La virtualidad a la cual se sujetan las relaciones sociales en sus múltiples ámbitos (social, político, económico, tecnológico, ambiental, militar, otros), dentro del escenario planteado en el ciberespacio, ha evolucionado significativamente y la tendencia seguirá intensificándose a una velocidad sorprendente. Esta evolución genera un debate acerca de cuan beneficiosa o perjudicial puede ser esta forma de relacionamiento social, dependiendo del enfoque desde el que se lo vea (Halpin, Trevorrow, Webb, & Wright, 2006, pág. 32).

  Por un lado los beneficios que nos han traído los avances en las redes informáticas son innegables ya que ahora se pueden hacer transacciones de toda índole de forma rápida y económica; la comunicación se ha agilitado y la información se encuentra al alcance de todos. Estos avances han facilitado la vida, pero al mismo tiempo han generado una dependencia creciente de tecnologías basadas en la información, y como no solo las redes lícitas han evolucionado sino también redes fraudulentas, todos nos encontramos en riesgo incluyendo las infraestructuras críticas tradicionales de un país (Halpin, Trevorrow, Webb, & Wright, 2006, pág. 32).

- Otro de los debates que gira en torno a las ciberamenazas y la ciberseguridad, se plantea en la siguiente pregunta: ¿hasta qué punto la ciberdefensa de un Estado es legítima, si utiliza instrumentos como el ciberespionaje, sobre los individuos de su propio país y de otros países? Se trata del debate entre la seguridad del Estado y la vulneración de los derechos de los ciudadanos, mediante el ciberespionaje, como lo vimos en los documentos que salieron a la luz, en el caso Snowden; se pudo apreciar que la mayoría de instituciones estatales de los Estados Unidos espiaba a sus ciudadanos, manejando información que, según Obama, era utilizada única y exclusivamente para la seguridad nacional.

> “En el Estado moderno, el individuo participa en el poder del Estado y a la vez tiene una esfera privada inviolable frente al poder del Estado, y en la que actúa su libertad.” (Pérez F. P., 2005, pág. 54)

Francisco Pérez nos deja ver cómo, teóricamente, el ciudadano tiene el derecho inviolable a su privacidad, sin embargo en el debate antes mencionado este derecho se pone en riesgo ya que se interfiere con la ciberseguridad del Estado.

- Las ciberamenazas son cada vez más importante para las políticas de seguridad y defensa de muchos países, ya que podría convertirse en un objetivo militar significativo en determinadas condiciones (Halpin, Trevorrow, Webb, & Wright, 2006, págs. 32-33). De modo1 que los Estados llevan a cabo ciberataques en respuesta a las ciberamenazas que se le presentan. El debate en este aspecto se presenta en cuanto a si sancionar al Estado que realiza el ciberataque en defensa propia o no hacerlo ya que un ataque en defensa propia no puede ser sancionado, en teoría, no debería ser sancionado, sin embargo atenta contra la seguridad internacional (Parks, 2013, pág. 73). Es decir que el país agresor debería ser castigado por actuar en contra de la seguridad internacional y generar inseguridad a otros países, pero este se ve amparado por actuar en defensa propia, lo que deja a cualquier sanción en el limbo.

CAPITULO 1

1. LA CIBERSEGURIDAD EN EL CONTEXTO GLOBAL Y REGIONAL

En el presente capitulo iniciaré con el análisis del contexto global de la ciberseguridad, mediante la presentación de los antecedentes fundamentales que han puesto a la defensa cibernética como prioridad para todos los Estados y la descripción de las dinámicas de ciberguerra que enfrenta el mundo. Posteriormente examinaré los elementos centrales de las respuestas que han dado los Estados frente a las ciberamenazas, tanto en forma individual, como a nivel multilateral. Finalmente presentaré el contexto regional de la ciberseguridad y las respuestas de los países latinoamericanos frente a las ciberamenazas, también a nivel individual y multilateralmente.

1.1. Contexto global de la ciberseguridad

1.1.1. Antecedentes fundamentales

Desde la creación del concepto de Estado, luego de la paz de Westfalia en 1648, ellos han tenido a su seguridad como uno de sus objetivos fundamentales, frente a la existencia de otros actores que representaban una amenaza (Buzan, Waever, & de Wilde, Security, A New Framework for Analysis, 1998).

En tal virtud, cada uno de los países ha visto la necesidad de desarrollar una estrategia para asegurar su subsistencia y proteger sus preciados bienes; así como también la soberanía de su territorio y a su población, de manera integral. Por ello cada una de sus maniobras estratégicas o las operaciones que realice, deben estar dirigidas a enfrentar cualquier amenaza, peligro o factor de riesgo, ya sea potencial o latente. Esta lógica de comportamiento representa desafíos permanentes para la concepción de la seguridad nacional,

puesto que en la medida en que un país aumenta su seguridad, genera inseguridad en los demás países, creándose así un círculo vicioso.

Hasta los años ochenta se veía al problema de la seguridad nacional principalmente desde la perspectiva realista, teoría que guiaba y daba una explicación del comportamiento de los actores, que se articulaba a un patrón básico orientado al desarrollo de sus capacidades militares para defender al Estado. En contraposición existía una fuerte incidencia de una perspectiva idealista, que pregonaba la paz entre los Estados, basada en los preceptos de la cooperación y las instituciones internacionales.

Con el fin de la guerra fría y de la estructura bipolar del sistema internacional de la posguerra a finales de los ochenta, era evidente que la seguridad se convertiría en un tema que debía ser repensado (Buzan, People, States & Fear: An Agenda for International Security Studies in the post-Cold War Era, 2008, pág. 4), ya que surgiría un nuevo sistema internacional, lo que supone nuevas amenazas. Desde este punto de vista la seguridad nacional toma un enfoque diferente puesto que la guerra se había trasladado también a un nuevo escenario conocido como el ciberespacio[6].

De acuerdo a lo que señala, Gema Medero en su artículo "La Ciberguerra", en 1990, con la Guerra del Golfo, se inicia la infoguerra, ya que se registran ataques cibernéticos, como por ejemplo la irrupción de aviones cargados con armas de precisión pertenecientes a una coalición internacional liderada por Estados Unidos y autorizada por la ONU, contra la red de telecomunicaciones y de energía de Bagdad[7].

[6] "El ciberespacio es un dominio caracterizado por el uso de la electrónica y el espectro electromagnético para almacenar, modificar e intercambiar información a través de sistemas de información en red e infraestructuras físicas." (Kuehl, 2009)

[7] "Aviones armados con municiones de precisión atacaron la red de telecomunicaciones y energía eléctrica de Bagdad, con especial saña contra los centros informáticos de la policía secreta iraquí. Además, según el Pentágono, un grupo de hackers holandeses se ofreció a Sadam para romper el sistema militar norteamericano en Oriente Medio." (Medero, LOS ESTADOS Y LA CIBERGUERRA, 2010, págs. 71-72)

Otro hecho que significó el inicio de la infoguerra en los años 90 fue el ataque por la red de internet que ejecutó el grupo guerrillero "Liberation Tigers of Tamil Eelam"[8], contra objetivos estadounidenses, mediante el lanzamiento de un "mailbombing"[9] a ordenadores gubernamentales (Medero, 2012, pág. 127). Con la actuación del grupo guerrillero LTTE podemos ver como los grupos ilegales también toman partido en la ciberguerra generando, una creciente inseguridad para los Estados.

En 1999, durante la guerra de Kosovo, expertos informáticos de diferentes nacionalidades atacaron a los computadores de la OTAN y de la Casa Blanca; también internet se llenó de páginas web con anuncios en contra tanto de Milosevic como de la OTAN (Medero, 2010, pág. 72). Estos ciberataques conectaron a la guerra que se estaba viviendo dentro de la ex Yugoslavia, con el exterior.

En la década del 2000 China empieza a sobresalir dentro de la infoguerra, ya que desde su territorio se propiciaron algunos ataques cibernéticos, entre los cuales está el que se considera como el más exitoso realizado contra la red del Departamento de Seguridad de los Estados Unidos. El sistema informático de la Cancillería Alemana, el Centro Nacional Informático de la India y las redes informáticas secretas de Nueva Zelanda y Australia también fueron atacados por China (Medero, 2010, pág. 73). Estos acontecimientos develan cómo los

[8] "Los Tigres de Liberación de Tamil Eelam (LTTE), son una organización guerrillera que buscaba establecer un estado Tamil independiente, Eelam, en el norte y el este de Sri Lanka. El LTTE creció hasta convertirse en uno de los grupos insurgentes más sofisticados y organizados del mundo. En marzo de 1990, los Tigres crecieron en fuerza y realizaron varias operaciones guerrilleras y ataques terroristas exitosos." (The Editors of Encyclopædia Britannica, 2015)

[9] Mail bomb: es el envío de una cantidad masiva de correos electrónicos a una persona o sistema específico. Una gran cantidad de correos puede simplemente llenar el espacio de disco del destinatario en el servidor o, en algunos casos, puede favorecer a que el servidor deje de funcionar. En el pasado, las bombas de correo se habían utilizado para "castigar" a los usuarios de Internet que han sido violadores flagrantes de la red de internet (por ejemplo, las personas que usan el correo electrónico para divulgar publicidad no deseada o spam). (TechTarget, 2007)

Estados utilizan ciberamenazas, como el ciberespionaje, para mantener su ciberseguridad[10] y su ciberdefensa[11].

Como muestra de que el ciberespionaje estaba en constante desarrollo, en el 2006 surge el sitio web Wikileaks, una página centrada en la publicación de documentos que contienen información confidencial acerca de temas religiosos, políticos, militares y sociales. Los documentos que hicieron que este sitio web se volviera tan mediático fueron aquellos que tenían que ver con los ataques indiscriminados del ejército estadounidense en Medio Oriente (Carrasco, INSTITUTO ESPAÑOL DE ESTUDIOS ESTRATEGICOS, 2010, págs. 1-2-3). Debido a la confidencialidad que ofrece este sitio, cualquier persona puede ser su informante sin ser descubierto, generando así un riesgo significativo a la seguridad cibernética de los Estados.

En el 2010 el mundo pudo ser testigo de las sofisticación con la que se estaban desarrollando las armas cibernéticas cuando una empresa bielorrusa llamada VirusBlokAda, descubrió el malware STUXNET[12], que tenía como objetivo principal atacar los sistemas industriales SCADA[13] , es decir que atacaba infraestructuras críticas tales como: plataformas petroleras, centrales eléctricas

[10] "Ciberseguridad: La seguridad cibernética es la recopilación de herramientas, políticas, conceptos de seguridad, medidas de seguridad, directrices, enfoques de gestión de riesgos, acciones, capacitación, mejores prácticas, aseguramiento y tecnologías que pueden utilizarse para proteger el entorno cibernético y la organización y los activos del usuario. Los activos de la organización y del usuario incluyen dispositivos informáticos conectados, personal, infraestructura, aplicaciones, servicios, sistemas de telecomunicaciones y la totalidad de la información transmitida y / o almacenada en el entorno cibernético. La seguridad cibernética se esfuerza por asegurar el logro y mantenimiento de las propiedades de seguridad de la organización y los activos del usuario frente a los riesgos de seguridad pertinentes en el entorno cibernético." (ITU, 2008, pág. 2)

[11] "Ciberdefensa: 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." (CARI, 2013, pág. 2)

[12] "Stuxnet es un gusano sofisticado diseñado para apuntar sólo a sistemas específicos de Siemens SCADA (control industrial). Este virus ataca a una vulnerabilidad de seguridad de una aplicación, antes de que los desarrolladores de la aplicación conozcan la vulnerabilidad. Y también utiliza, técnicas avanzadas para ocultarse de los usuarios y del software anti-malware, tanto en Windows como en los equipos de control a los que apunta." (Mueller & Yadegari, 2012)

[13] "El sistema SCADA hace referencia a un sistema de adquisición de datos y control supervisor. Tradicionalmente se lo define como un sistema que permite supervisar una planta o proceso por medio de una estación central que hace de Master y una o varias unidades remotas por medio de las cuales se hace el control y la adquisición de datos hacia y desde el campo." (Corrales, 2007)

y centrales nucleares, y las saboteaba. Este virus infectó mayoritariamente a sistemas industriales en Irán, incluyendo su planta de enriquecimiento de combustible, por lo que se hablaba de que el objetivo de STUXNET era llegar a atacar también las instalaciones nucleares del país, lo cual se confirmó posteriormente cuando el presidente iraní, Mahmoud Ahmadinejad, aseguró que un virus había causado problemas a algunas de las centrifugadoras nucleares (Shakarian, 2012, pág. 50). Este gusano informático marcó un antes y un después en cuanto a los ciberataques ya que nunca antes se había visto un arma cibernética que infectara y dañara estructuras criticas industriales de un país, lo que representaba un adelanto impresionante en el diseño de malware.

La actual situación de riesgo en el ciberespacio depende mayoritariamente de la apertura y la accesibilidad de las redes informáticas con que cuenta un país. El internet es la red informática más grande y la que da mayor apertura al usuario en el mundo, por lo que es susceptible y puede facilitar eventos criminales y fraudulentos (Beissel, 2016, pág. 1). Es por esta razón que cualquier sistema que se encuentre conectado a internet, como por ejemplo las redes eléctricas inteligentes, la computación en nube, las redes de automatización industrial, los sistemas de transporte inteligentes, la ciberadministración y la banca electrónica, están amenazados por masivos ataques en la web. Pues como lo señala Duart en su artículo “Educar en valores en entornos virtuales de aprendizaje: realidades y mitos”:

> “los nuevos significados que genera la realidad de los entornos virtuales nos conduce a entender la virtualidad como un espacio creativo (en Levy, 1999), como algo que genera situaciones distintas que hasta ahora no existían. Lo que cambia en la virtualidad es sobre todo el potencial comunicativo, la interacción. La virtualidad establece una nueva forma de relación entre el uso de las coordenadas de espacio y de tiempo. La virtualidad supera las barreras

> espacio temporales y configura un entorno en el que la información y la comunicación se nos muestran asequibles desde perspectivas hasta ahora desconocidas al menos en cuanto a su volumen y posibilidades". (Duart, 2008, parr. 9)

Paralelamente al desarrollo de la tecnología, se incrementan las actividades criminales y fraudulentas en el entorno que otorga el ciberespacio, y no solo se han incrementado en cantidad, sino también en sofisticación lo que las hace más peligrosas y complejas. Los hackers, cuando atacan a una empresa privada o pública ya no toman en cuenta únicamente al sistema informático y sus debilidades, también analizan características especiales de la empresa, como lo son su infraestructura y sus trabajadores. Por esta razón en la actualidad tanto las empresas como las personas son vulnerables ante los ataques cibernéticos y pueden ser afectadas gravemente, lo que genera un sentimiento de inseguridad frente a la imposibilidad de actuar individual o colectivamente para proteger sus derechos.

El creciente conocimiento y accionar de los hackers los ha convertido en otro "sector económico", ya que mediante un software malicioso pueden robar grandes cantidades de dinero, proyectos valiosos y manipular información sensible de los individuos, afectando así a sectores críticos de un Estado. La amenaza más grande surge del hecho de que las agrupaciones de hackers son altamente organizadas y han diseñado sus técnicas de forma muy comprensible, para que la mayoría de personas pueda utilizarlas, de manera que se propaguen los ciberataques.

1.1.2. Ciberguerra

Desde la perspectiva de Richard Stiennon en su libro "Surviving Cyberwar" (Stiennon, 2010), desde los años 90 ya se avizoraba un conflicto debido al pensamiento político-militar de China, el surgimiento de la ciberdelincuencia, la omnipresencia de internet, la revolución de los satélites soviéticos y la

evolución de los malware. Pero en el 2001, este conflicto se hace inminente, cuando una aeronave estadounidense, denominada E3, patrullaba las costas de China con la misión de interceptar y recolectar información sobre el tráfico de comunicaciones militares, comerciales y gubernamentales de China, que iba a ser analizada por expertos de inteligencia de la Agencia de Seguridad Nacional de Estados Unidos. Durante su patrullaje de rutina, el E3 fue interceptado por un avión de combate Chino. El piloto Wu Nos llevó a su avión en curso de colisión contra el desarmado E3 sacándolo del aire (Stiennon, 2010, pág. 12). Esto evitó que el avión estadounidense cumpliera su cometido y robara información clasificada del gobierno Chino.

Este hecho desencadenó un choque diplomático tan fuerte que solo puede ser comparado con lo ocurrido el 1960 cuando el avión espía estadounidense U-2 fue derribado por un misil soviético. Aquí no existía algo secreto, tanto los chinos como los estadounidenses sabían que la misión de E3 era robar información e interceptar sus redes y que fue un avión chino el que interceptó al E3, por lo que Estados Unidos exigió el regreso de su aeronave y su tripulación; China por su parte exigió una disculpa de los Estados Unidos.

El 26 de Abril 2001 China anunció que hackers chinos iban a librar una guerra cibernética durante siete días, como autodefensa en contra sitios web norteamericanos por lo ocurrido con el E3; los objetivos principales incluían a cientos de sitios web gubernamentales y militares de Estados Unidos. Esta guerra fue coordinada por el gobierno Chino para testear la ciberdefensa de Estados Unidos y para medir su capacidad de respuesta diplomática, militar y económica, en caso de una intrusión en sus sistemas. No existió ningún tipo de respuesta por parte de los Estados Unidos, ningún diplomático lanzó una advertencia, no hubo amenaza de invasión de territorio, y tampoco hubo ninguna respuesta militar.

Más o menos en el 2003 China empieza a incursionar en el espionaje cibernético industrial. En el 2005 Shaw Carpenter, un veterano norteamericano

de la marina, realizó una investigación acerca del espionaje chino o el Titan Rain[14], pero todos los eventos que se encontraron en la investigación eran nada más la punta del iceberg. China ha estado invadiendo sistemáticamente ámbitos públicos y privados, y robando los recursos informáticos de casi todo el mundo; lamentablemente la mayor cantidad de sus objetivos están desprotegidos ante este espionaje.

Mientras China y EEUU se encontraban activamente estudiando la guerra cibernética y reorganizando sus jerarquías militares para dar cabida a un nuevo campo de combate, las verdaderas innovaciones en cuanto a ciberataques se estaban dando en otras regiones y con otros actores. Se estaba iniciando la participación de la delincuencia organizada en el ciberespacio, y de organismos terroristas que se podían beneficiar en gran medida de armas informáticas (Stiennon, 2010, pág. 51). Podemos ver como se complejiza la ciberguerra ya que no solo los Estados están inmiscuidos en ello, sino también grupos con etnias o religiones diferentes.

Para Stiennon hay tres puntos de calor o "hot spots" preocupantes, que revelan un nuevo desarrollo de la ciberguerra, ellos son: Israel contra Hamas[15], Siria[16], Irán[17], Pakistán contra la India[18] y Corea del Norte contra

[14] "Shawn Carpenter era un analista de seguridad para Sandia National Laboratories, donde buena parte del arsenal nuclear estadounidense es diseñado. Sin embargo, en su tiempo de descanso se dedicaba a perseguir a un grupo de ciberespías chinos desde su casa, bajo el nombre clave que sus empleadores del departamento de inteligencia militar le dieron: Spiderman. El grupo de hackers que Carpenter estaba rastreando fueron nombrados por los investigadores federales como Titan Rain y captaron su atención por primera vez en septiembre de 2003, cuando estuve investigando una irrupción en los sistemas de Lockheed Martin, muy similar a otro ataque dirigido a Sandia un par de meses después." (Barrueto, 2009)

[15] "Durante la acción militar de enero de 2009 en Gaza, los ataques contra sitios web israelíes y estadounidenses se convirtieron en otro ejemplo de un ataque cibernético masivos. Decenas de atacantes sistemáticos configuraron más de 800 sitios web con mensajes pro-Hamas, muchos de ellos representando imágenes espantosas de bebés muertos y civiles heridos. Entre los sitios atacados estaban los sitios de noticias israelíes, los servidores del gobierno, e incluso los hospitales que trataban a las víctimas palestinas de la guerra de Gaza. En retaliación a esto por lo menos un sitio web israelí publicó instrucciones para atacar sitios web de Hamas." (Stiennon, 2010, pág. 77)

[16] "En noviembre de 2009, Spiegel Online publicó la historia de la destrucción de la instalación nuclear siria. Un alto funcionario sirio se registró en un hotel en Londres. Estaba bajo observación del Mossad, la agencia encubierta de Israel. Cuando dejó su computadora portátil desatendida en su habitación de hotel, los israelíes entraron en su habitación y colocaron un caballo de Troya sobre él. Spiegel Online revela que había muchos documentos extraídos de esa computadora portátil que demostró la existencia de una

Core del Sur[19] (Stiennon, 2010, págs. 52-53). Estos conflictos son continuamente analizados por otro Estados, ya que la supervivencia dentro de la ciberguerra depende del aprendizaje que se adquiera de cada una de estas disputas.

En el 2006 aparecen involucradas organizaciones no gubernamentales en la ciberguerra con el caso WikiLeaks, que es una organización sin fines de lucro fundada por Julian Assange, que publica informes y documentos de carácter confidencial, sobre aspectos sensibles de índole militar, política, religiosa o social mediante un sitio web (Carrasco, 2010, pág. 1).

En los años siguientes se dieron millones de ciberataques, pero en el 2013 detona otra bomba en el ambiente de la ciberguerra, es el caso Snowden en el que Edward Snowden, consultor tecnológico estadounidense y trabajador de la CIA, filtró más de 20.000 documentos sensibles o clasificados, sustraídos de los servidores de la National Security Agency (NSA) de Estados Unidos (Real Instituto Elcano, 2013, pág. 1). Sobre estos hechos se puede reflexionar que, de acuerdo a la información que ha sido publicada, Estados Unidos ha generado políticas, estrategias, tácticas, maniobras y ha asignado medios y recursos para poder realizar ciberataques y neutralizar posibles amenazas en el ciberespacio.

---

instalación de investigación nuclear en la puerta de Israel. La información robada de esta computadora portátil dio a Israel evidencia de la instalación de investigación nuclear de Siria. Israel bombardeó esa instalación en septiembre de 2006, y Siria destruyó y pavimentó los restos para esconder las pruebas." (Stiennon, 2010, pág. 54)

[17] "Irán ha disparado misiles balísticos de gama media y continúa refinando materiales como ojivas nucleares para armar esos misiles, lo cual lo hace vulnerable ante las ciberamenazas y le obliga a avanzar en el uso de tecnologías e internet." (Stiennon, 2010, pág. 52)

[18] "Ambos forman parte del club nuclear lo que ha frenado en gran medida los ataques cibernéticos pero el 17 de noviembre de 2008, el sitio web de la Autoridad Reguladora de Petróleo y Gas de Pakistán fue desconfigurado por un grupo indio de destrucción llamado Hindu Militant Group. Para el 24 de noviembre de 2008, un grupo pakistaní de desconfiguración llamado Pakistan Cyber Army surgió y respondió a la desconfigurando el sitio web de la Corporación de Petróleo y Gas Natural de la India." (Stiennon, 2010, págs. 55-56)

[19] Estados Unidos y Corea del Sur se han unido para mejorar sus capacidades de respuesta frente a la amenaza cibernética que representa Corea del Norte. Se le han atribuido a Corea del Norte varios ataques cibernéticos a Corea del Sur a pesar de no contar con las pruebas suficientes. (Stiennon, 2010, pág. 58)

Sin embargo en el 2016 se registró la filtración documental de mayor alcance en la historia, con los denominados “Panamá Papers”, con información de grandes empresas, sobre acciones y conversaciones de primeros ministros, dictadores, jeques, emires, reyes, amigos de reyes, la mafia, traficantes, capos de la droga, agentes secretos, directivos de la FIFA, aristócratas y famosos, es decir de gente que poseía mucho dinero pero que lo tenía depositado en paraísos fiscales. Según el analista político internacional Jorge Kreiner (telesur, 2016), el objetivo que perseguía Estados Unidos con la publicación de estos documentos era el desprestigio a Vladimir Putin, ya que estos documentos lo vinculaban, y el control de los fondos que se encontraban depositados en estos paraísos fiscales; tanto bancos de New York como de Londres tienen un convenio con las Bahamas para transferirles sus fondos.

Los hechos antes mencionados son los más relevantes y conocidos dentro de la ciberguerra pero no son los únicos. En la actualidad existen páginas web como NORSE, donde se pueden ver los ciberataque en tiempo real y se pueden contabilizar al menos 50 ciberataques por minuto, lo que complejiza el hecho de detallar cada uno de los ataques cronológicamente y desde que lugar se realizó, sin embargo nos ayuda a entender por qué se habla de una ciberguerra y la naturaleza anárquica que predomina en el ciberespacio.

1.1.3. Respuestas de los Estados frente a las Ciberamenazas

Las respuestas que analizaremos son Estatales, es decir que nos enfocaremos en ver cuáles son las instituciones estatales que se encargan de la ciberseguridad del país, de qué manera se gestionan los incidentes informáticos y si cuentan con programas para desarrollar las capacidades del Estado en materia de ciberdefensa.

1.1.3.1. Respuestas individuales

Cabe mencionar que se analizaran en el contexto global las respuestas individuales de los países desarrollados que más ciberataques reciben, lo que genera respuestas más amplias y diversas.

1.1.3.1.1. Estados Unidos

Para examinar las respuestas que han dado los Estados Unidos tomare como referencia a Gian Piero Siroli, citado en el libro "Cyberwar, Netwar and the Revolution in Military Affairs" (Halpin, Trevorrow, Webb, & Wright, 2006).

Estados Unidos posee el ejército más fuerte del mundo y la economía nacional más grande. El financiamiento de estas dos dimensiones y su poder, dependen cada vez más de ciertas infraestructuras críticas y de sistemas de información basados en el ciberespacio[20], por lo que son mucho más vulnerables ante ataques cibernéticos. Esto se demuestra con todos los ciberataques que ha recibido históricamente. Ante esta Guerra Informática (IW), el gobierno ha llevado a cabo diversas actividades y programas de investigación, centrándose en cuestiones de protección, seguridad y supervivencia de las infraestructuras vitales del país.

En 1995, el Secretario de Defensa de los Estados Unidos formó la Junta Ejecutiva de la Guerra de la Información con el objetivo de desarrollar y alcanzar objetivos nacionales en cuanto a Seguridad Nacional frente a la IW. En el mismo año, la Directiva sobre las Decisión Presidencial estableció políticas relacionadas principalmente con las amenazas terroristas, que incluyen al ciberterrorismo (Halpin, Trevorrow, Webb, & Wright, 2006, pág. 33).

[20] "Debido a nuestra fuerza militar, los futuros enemigos, ya sean naciones, grupos o individuos, pueden tratar de perjudicarnos de maneras no tradicionales, incluyendo ataques dentro de los Estados Unidos. Debido a que nuestra economía depende cada vez más de infraestructuras interdependientes y con soporte cibernético, los ataques no tradicionales a nuestra infraestructura y sistemas de información pueden ser capaces de dañar significativamente tanto nuestro poder militar como nuestra economía." (Presidential Decision Directives (PDD63), 2016, parr. 3)

En 1996, la Orden Ejecutiva 13010 creó la Comisión Presidencial sobre Protección de Infraestructura Crítica (PCCIP), para evaluar las amenazas físicas y cibernéticas que podrían afectar infraestructura vital de modo que se pueda desarrollar estrategias de protección (Halpin, Trevorrow, Webb, & Wright, 2006, pág. 33). También se creó el Grupo de Trabajo sobre Protección de Infraestructura, que tenía como función coordinar actividades para proteger las infraestructuras sensibles.

En la Directiva de Decisiones Presidenciales 63 (PDD63), de 1998, se incluyeron factores clave para la política estadounidense sobre protección de infraestructuras críticas[21]. Poco después se creó el Centro Nacional de Protección de Infraestructuras (NIPC) en el FBI y la Oficina de Aseguramiento de Infraestructura (CIAO) en el Departamento de Comercio. En este año también se puso en marcha el proyecto de la Red Federal de Detección de Intrusiones (FIDNet), para resguardar al Estado y a las empresas clave del sector privado, a través de un amplio monitoreo de sistemas y redes.

La Orden Ejecutiva 13130 estableció el National Infrastructure Assurance Council (NIAC) en 1999. Posteriormente, en el 2000, la administración estadounidense publicó un Plan Nacional de Protección de Sistemas de Información, en el que se detallaban las nuevas dependencias y amenazas que enfrentaba el país. En este plan se propuso una asociación público-privada de capacitación sobre la defensa cibernética y la FIDNet (Halpin, Trevorrow, Webb, & Wright, 2006, pág. 34). Sin embargo la iniciativa FIDNet fue desechada y reemplazada en años posteriores.

[21] Factores Clave: (Presidential Decision Directives (PDD63), 2016)

- "El presidente estadounidense manifestó su intención de que los Estados Unidos tome todas las medidas necesarias para eliminar rápidamente cualquier vulnerabilidad significativa tanto a ataques físicos como a ataques cibernéticos en sus infraestructuras críticas, incluyendo especialmente a los sistemas cibernéticos."
- "Se planteó un objetivo nacional en el que se esperaba que a más tardar en el año 2000, los Estados Unidos alcanzaran una capacidad operativa inicial y, a más tardar dentro de cinco años posteriores , los Estados Unidos esperaban lograr y mantener la capacidad de proteger las infraestructuras críticas del país de actos intencionales"
- "Se propone un alianza público-privada para reducir la vulnerabilidad"

En el 2002 la Junta de Protección de Infraestructura Crítica emitió un informe sobre la estrategia nacional para asegurar el ciberespacio y el Comité Económico Conjunto del Congreso, publicó un documento con el título "La seguridad en la era de la información", en el que se puntualizaban algunos aspectos sobre la protección de la infraestructura crítica (Halpin, Trevorrow, Webb, & Wright, 2006, pág. 34). Desde entonces muchas actividades enmarcadas en esta temática se han desarrollado en los Estados Unidos.

Entre el 2011 y el 2014 se han generado iniciativas tales como: "la mejora de la ciberseguridad de infraestructuras críticas", "la seguridad de Infraestructuras críticas y su resiliencia[22]", "reformas estructurales para mejorar la seguridad de las redes y el intercambio responsable para salvaguardar la información clasificada" (The White House, 2015) . En la actualidad la responsabilidad acerca de la ciberseguridad de los Estados Unidos está distribuida entre varias entidades; sin embargo el principal responsable de la coordinación de políticas cibernéticas es el Comité de Política e Inteligencia de Infraestructura de Información y Comunicaciones (ICI-IPC) del Consejo de la Casa Blanca. El ICI-IPC está regido por el Consejo de Seguridad Nacional y el Coordinador de Seguridad Cibernética (CSC). El CSC se encarga principalmente de liderar el desarrollo de la estrategia y de la política nacional de ciberseguridad. (Pernik, Wojtkowiak, & Verschoor-Kirss, 2016, págs. 15-16)

El Departamento de Seguridad Nacional es la institución encargada de la ciberseguridad dentro de las fronteras de EEUU. Sus principales funciones son: fortalecer la ciberseguridad y la resiliencia de las infraestructuras críticas, ayudar a las agencias civiles federales con respecto a la inversión en ciberseguridad, y garantizar un ambiente cibernético saludable. (Pernik, Wojtkowiak, & Verschoor-Kirss, 2016, pág. 16)

[22] Resiliencia: La resiliencia según Luthar es "la manifestación de la adaptación positiva a pesar de significativas adversidades de la vida". (Becoña, 2006, pág. 128)

Durante la presidencia de Barak Obama, aumentó la concientización acerca del riego que representan las ciberamenazas a la seguridad nacional. Una de las primeras medidas que se tomaron dentro de su periodo presidencial fue encargar una revisión, que duró 60 días, de las directivas, políticas y acciones que se estaban llevando a cabo hasta el momento, para definir una estrategia que reforzara la seguridad y sus capacidades tanto defensivas como ofensivas en el ciberespacio. Esto tuvo como resultado la creación de un comando militar que continuamente está desarrollando sus capacidades para reaccionar en caso de que las estructuras críticas se encuentren amenazadas. (Acosta, Rodriguez, Ballesteros, & Taboso, 2009, pág. 31)

1.1.3.1.2. China

En China se ha visto desde 1993, al internet como una oportunidad para su modernización, por lo que el gobierno chino ha formulado una serie de políticas para su desarrollo en internet y para promover la informatización de la sociedad. En 1997 el país asiático elaboró el Programa Nacional de informatización[23] en el que se incluyó al internet en la construcción de la infraestructura nacional y en el proceso de informatización de la economía nacional para desarrollar su industria en la red (Ventre, 2014, págs. 5-6).

En el año 2002 el Congreso Nacional propuso impulsar la industrialización a través de la informatización y para el año 2006 ya se discutía en la Asamblea Nacional de una estrategia para fusionar las redes de difusión con el internet y acelerar su aplicación comercial (Ventre, 2014, págs. 6-7), es decir, se quería comercializar sus productos por medio de páginas web. Desde el año 2006 China vio el potencial comercial que tenía el internet por lo que lo utilizo para llegar a ser un hegemón[24] en el ciberespacio, ya que en la actualidad existen un sin número de páginas web chinas mediante las cuales venden sus

[23] Informatización: "Implantación o aplicación de medios informáticos para el desarrollo de una actividad o trabajo." (Oxford Living Dictionaries, 2016)

[24] Hegemon: "Un líder, país o grupo, que es muy fuerte y poderoso y por lo tanto capaz de controlar a otros" (Cambridge Dictionary, 2017)

productos alrededor del mundo; páginas web de otras nacionalidades también comercializas productos chinos de toda índole.

En el 2010 el Consejo de Estado decidió acelerar la fusión de las redes de difusión con el internet para avanzar en la industria cibernética. Debido a este tipo de estrategias el desarrollo, en el uso de internet, que ha tenido China ha sido integral, sostenible y rápido hasta la actualidad, lo cual las vuelve sensibles ante las ciberamenazas. El gobierno chino tiene la responsabilidad de proteger por ley los derechos, intereses y la seguridad de los ciudadanos chinos; esto incluye el ciberespacio. Para lograrlo el Estado ha establecido diferentes órganos gubernamentales para realizar este trabajo. El departamento de administración de telecomunicaciones nacionales es responsable de la administración de la industria de internet (Ventre, 2014, pág. 13).

Dentro de marco de un plan integrado, el People's Liberation Army (PLA)[25] de China ha enunciado una doctrina oficial en materia de ciberguerra, que contempla un entrenamiento adecuado para sus oficiales llevando a cabo simulaciones de ciberguerra y ejercicios militares. El servicio de inteligencia de Beijín se encarga de recolectar información científica y tecnológica para alcanzar las metas del gobierno, mientras que la industria china se encarga de ofrecer productos tecnológicos para la ciberseguridad del Estado. El PLA también maneja los lazos que existen entre China y Rusia en el ciberespacio (Acosta, Rodriguez, Ballesteros, & Taboso, 2009, pág. 36). En China, el Ejército de Liberación Popular ha constituido el Centro de Guerra de la Información, ya que dirige las acciones en relación a la infoguerra (Medero, Dialnet, 2012, pág. 66).

China cuenta con un comando especial de 30 soldados, llamados "Ejercito Azul", entrenados para mejorar la ciberseguridad del país y proteger a las

[25] "El Ejército Popular de Liberación es una organización unificada de las fuerzas terrestres, marítimas y aéreas de China. Es una de las fuerzas militares más grandes del mundo." (The Editors of Encyclopædia Britannica, 2017)

redes militares de ciberataques (Lewis, 2011). Su misión es estudiar la seguridad de las redes y ordenadores para proporcionar servicios de respuesta a las víctimas de ataques informáticos y publicar las alertas relativas a amenazas y vulnerabilidades (Medero, Dialnet, 2012, pág. 66).

1.1.3.1.3. Rusia

En el año 2000 la Federación Rusa formuló una doctrina de seguridad de la información, que describe las diferentes amenazas que enfrenta la nación dentro del ciberespacio y cómo debería actuar el Estado para proteger su información estratégica. (Lemieux, 2015, pág. 70).

En esta lógica el ejército ruso considera que las afectaciones que causan las armas informáticas dentro de la ciberguerra son comparables con las de las armas nucleares, por lo que, si dentro de este conflicto se ven afectados sistemas de mando y control económico a nivel nacional o la capacidad de combate del ejército, Rusia se reserva el derecho de utilizar armas nucleares contra armas de información reales; por lo tanto las fuerzas armadas rusas han desarrollado principios y reglas para la protección de los sistemas críticos del país, y también para la disuasión y prevención de ataques cibernéticos. Según los representantes del régimen de Putin, Rusia tiene la capacidad de actuar globalmente y el derecho de usar todos los medios posibles para proteger sus sistemas críticos (Lemieux, 2015, pág. 72).

1.1.3.1.4. Israel

Israel hasta la actualidad ha sido blanco de ciberataques a gran escala, por lo que ha generado una doctrina para responder a tales amenazas, la cual no se centra únicamente en los sistemas y la tecnología avanzada de defensa cibernética, sino también en el desarrollo de técnicas interdisciplinarias que integre a los laboratorios nacionales de investigación militar, a las unidades de

inteligencia, a las organizaciones sin fines de lucro, a la Oficina Cibernética Nacional y a las empresas y empresarios amateurs (Raska, 2015, pág. 5).

Raska destaca que la estrategia de Israel pretende aprovecha sistemas computarizados automatizados y personal altamente capacitado, para combinar inteligencia, prevención temprana, defensa activa y pasiva, y capacidades ofensivas, tanto a nivel civil como militar.

A menudo se atribuye a la Fuerza de Defensa Israelí (FDI), la creación y el éxito de la industria de la tecnología de punta del país, en vista de que la FDI concentra el núcleo de las capacidades de defensa cibernética y maneja la selección, capacitación, investigación y desarrollo de habilidades de los defensores cibernéticos.

1.1.3.1.5. Alemania

El gobierno alemán considera que las estructuras de la información son tan importantes para el país como las carreteras, el agua, o el suministro eléctrico. Por esta razón Alemania cuenta con un Plan Nacional para la Protección de la Infraestructura de Información (NPIIP), que protege la información crítica, de amenazas globales. (Acosta, Rodriguez, Ballesteros, & Taboso, 2009, pág. 33)

En este sentido el NPIIP tiene tres objetivos principales que son: la prevención para poder proteger las infraestructuras críticas de forma adecuada; la preparación para responder efectivamente ante los ataques cibernéticos; y la sostenibilidad, que les ayudará a mejorar las competencias de Alemania en cuanto a las tecnologías de la información.

1.1.3.1.6. Reino Unido

Luego de los ataques terroristas del 7 de julio de 2005[26] , el Reino Unido ha incluido en su Plan de Seguridad Nacional, como aspecto prioritario, a la protección de infraestructuras críticas del país. El gobierno inglés considera que el internet es parte de las infraestructuras críticas, puesto que puede ser usado por terroristas, criminales y naciones hostiles. (Acosta, Rodríguez, Torre, Ballesteros, & Taboso, 2009, págs. 31-32)

Para conseguir los objetivos que se persiguen en el Plan de seguridad Nacional, con respecto a la ciberdefensa, se han tomado acciones como: crear el Centro para la Protección de las Infraestructuras Nacionales, como resultado de la fusión del centro encargado de informar acerca de la seguridad en redes e información, y del centro encargado de la seguridad de las instalaciones y del personal. También ha desarrollado una Estrategia Nacional de Seguridad de la Información, dentro del Programa Técnico de Seguridad de la Información, y la lucha contra el crimen. (Acosta, Rodriguez, Ballesteros, & Taboso, 2009, pág. 32; Acosta, Rodriguez, Ballesteros, & Taboso, 2009)

Los países han respondido individualmente, de acuerdo a sus capacidades (económicas y tecnológicas), ante las amenazas cibernéticas más frecuentes, creando instituciones especializadas en ciberseguridad y defensa, capacitando a su personal, generando carreras universitarias en materia de seguridad cibernética para desarrollar talento humano, concientizando a sus ciudadanos frente a las ciberamenazas y el uso seguro del internet, y buscando la cooperación en entre el sector privado y público. También han utilizado la disuasión y la prevención para hacerle frente a las ciberamenazas. Igualmente han generado diversas iniciativas y propuestas a nivel multilateral.

1.1.3.2. Respuestas Multilaterales

[26] Referirse: Frank Gregory (2006). Los atentados de Londres del 7 y 21 de julio de 2005: ¿una "nueva normalidad" o lo ya previsto?

Se analizarán muy brevemente las respuestas multilaterales generadas por las organizaciones internacionales más grandes a nivel global, con más relevancia y que han implementado programas que buscan promover mejores niveles de ciberseguridad para sus miembros.

1.1.3.2.1. Naciones Unidas

En 1990, la Asamblea General de la ONU estableció normativas para la regulación de los archivos de datos personales. Esta medida destacaba la importancia de la protección de datos, no solamente en los países industrializados sino en todo el mundo. (Weber & Heinrich, 2012, pág. 25)

La ONU como organismo internacional de mayor membresías, ante el fenómeno cibernético que enfrenta la sociedad mundial y los Estados, continuamente está repensando las normativas y la política pública internacional, para entender mejor esta amenaza global y posicionarse en este campo con mayor efectividad. La ONU tiene entre los organismos responsables del tema de la ciberseguridad a la Unión Internacional de Telecomunicaciones (UIT), que se ha unido a la Alianza Internacional Multilateral contra las Ciberamenazas (AINCA/ IMPACT), para promover el comportamiento seguro en línea y una respuesta multilateral efectiva ante estas amenazas (ITU, Unión Internacional de Telecomunicaciones, 2007).

La ONU pretende apoyar a los países miembros; pero ello también puede generar inseguridad en otros países que se ven en la necesidad de generar alianzas y estrategias para defenderse, incrementando la inseguridad y el conflicto.

El 9 de Diciembre del 2014 la UIT publicó el Global Cybersecurity Index, que evalúa el compromiso de cada uno de los países miembros con la ciberseguridad; la evaluación se realizó tomando en cuenta los siguientes aspectos en cada nación: medidas legales, medidas técnicas, medidas

orgánicas, capacitación frente a las necesidades de la ciberdefensa, cooperación y establecimiento un CERT (Morán, 2015). En base a la tabla que se generó de esta investigación, el UIT puede llevar a cabo programas de ciberseguridad más efectivos en base a las capacidades de cada país.

1.1.3.2.2. OTAN

La OTAN ha implementado iniciativas de defensa inteligente para que los países miembros puedan desarrollar, en conjunto, sus capacidades con respecto a la ciberseguridad. Ello incluye la creación de la Plataforma de Intercambio de Información sobre Malware (MISP), el proyecto de Desarrollo de Capacidades Multinacionales de Defensa Cibernética (MN CD2) y el proyecto Multinacional de Educación y Capacitación en Ciberdefensa (MN CD E & T). (OTAN, 2017)

También está mejorando sus capacidades con respecto a la educación cibernética y la capacitación, para ayudar a que los Estados miembro generen conciencia acerca de las ciberamenazas y de los riesgos que representa el cieberespacio.

“El Centro de Excelencia Cooperativa de Ciberdefensa de la OTAN (CCD CoE) en Tallin, Estonia es la principal institución de investigación y capacitación acreditada por la OTAN, que se ocupa de la educación, la consulta, las lecciones aprendidas, la investigación y el desarrollo de la ciberdefensa.” (OTAN, 2017)

“La Escuela de Sistemas de Información y Comunicaciones de la OTAN (NCISS) en Latina, Italia, imparte capacitación a personal de naciones aliada, con respecto al funcionamiento y mantenimiento de los sistemas de comunicación e información de la OTAN. La Escuela OTAN en Oberammergau, Alemania, realiza actividades de educación y formación, relacionadas con la defensa cibernética, para apoyar las operaciones, la

estrategia, la política, la doctrina y los procedimientos de la alianza. El Colegio de Defensa de la OTAN en Roma, fomenta el pensamiento estratégico sobre asuntos político-militares, incluso en cuestiones de defensa cibernética." (OTAN, 2017)

Las medidas que ha tomado la OTAN en materia de ciberseguridad, evidencian que el papel de esta organización es crucial en el sistema internacional, ya que por un lado busca proteger sus propias redes, lo cual implica que sus sistemas de información estén protegidos frente a ciberamenazas, y por otro lado ayuda a que los países miembro desarrollen sus propias capacidades de ciberdefensa mediante el establecimiento de metas colectivas que cada aliado debe firmar y comprometerse a cumplir.

Otro aspecto destacado es el mecanismo de ayuda para los países miembros, incluyendo la formación que ofrecen las instituciones educativas antes mencionadas. Todo esto tiene una razón de ser, y es que las capacidades que posee la alianza para realizar tareas de defensa colectiva dependen netamente de las capacidades de cada uno de los aliados.

Las organizaciones internacionales buscan una gobernanza electrónica conjunta, mediante la cooperación internacional, de modo que todos sus miembros puedan mejorar sus capacidades dentro del ciberespacio y desarrollar su ciberseguridad de la mejor manera. Las organizaciones internacionales cuentan con marcos normativos bajo los cuales se deberían regir todos sus miembros y también llevan a cabo iniciativas para concientizar acerca de las ciberamenazas.

1.2. América Latina Frente a la Ciberamenazas

1.2.1. Contexto Regional

Los cibercrímenes originados y orientados hacia los países y las economías de América Latina, al igual que hacia el resto del mundo, están aumentando ya que es el cuarto mayor mercado en el mundo y la mitad de su población utiliza internet (AETecno, 2016).

Existe un gran número de redes cibernéticas criminales y de delincuencia organizada en la región, mismas que no han podido ser controladas debido a la ineficacia del sistema de aplicación de la ley y a la debilidad de sus instituciones. Esto ha causado que la banca en línea de América Latina se convierta en un objetivo atractivo para la ciberdelincuencia. Tanto el sector público como el sector privado carecen de sistemas y procedimientos necesarios para defenderse (Kshetri, 2013, pág. 135), ya que en la región se están implementando nuevas tecnologías de la información sin tomar en cuenta las medidas de seguridad.

Por ejemplo, en el 2006 se calculó que en Brasil alrededor de 3 millones de medianas y pequeñas empresas no contaban con un antivirus en sus computadoras y que las páginas oficiales de los gobiernos de Ecuador, Venezuela y Colombia habían sido utilizadas para enviar virus. (Kshetri, 2013, pág. 140).

Las tres fuentes principales de phishing[27] en América Latina son Brasil, Colombia y Argentina; estos tres países representan el 74% de phishing en la región y el 3.2% a nivel mundial (Organización de los Estados Americanos, 2014, pág. 14). Según un informe reciente del Banco Interamericano de Desarrollo (BID), los países latinoamericanos, se encuentran poco preparados para contrarrestar las amenazas cibernéticas. Esto se debe a que estos países no dimensionan los daños que pueden ocasionar estas amenazas, lo cual

[27] "El phishing es una técnica de ingeniería social utilizada por los delincuentes para obtener información confidencial como nombres de usuario, contraseñas y detalles de tarjetas de crédito enviando correos electrónicos que aparentan venir de fuentes confiables como por ejemplo entidades bancarias." (SeguInfo, 2016)

hace que tengan respuestas muy limitadas y parciales. (Banco Interamericano de Desarrollo, 2016).

A pesar de todos los indicadores de que Latinoamérica es un blanco de los ciberataques, en la región no todos los gobiernos han tomado a la ciberseguridad como un aspecto prioritario de la seguridad nacional, los Estados de la región que han adoptado estrategias relevantes de seguridad cibernética son: Brasil, Colombia, Argentina y Chile.

La sociedad también desconoce el riesgo que implica el uso de las tecnologías de la información (OBSERVATORIO DE LA CIBERSEGURIDAD EN AMÉRICA LATINA Y EL CARIBE, 2016, pág. 115). Esto, conjuntamente con el crecimiento acelerado de la conectividad y la dependencia del internet, aumenta la vulnerabilidad de la región.

1.2.2. Respuestas de los gobiernos Latinoamericanos

1.2.2.1. Respuestas individuales de países Latinoamericanos

Se analizarán las respuestas de los países latinoamericanos, antes mencionados, que han adoptado estrategias relevantes de ciberseguridad en la región.

1.2.2.1.1. Argentina

Para analizar y exponer las respuestas de Argentina frente a las ciberamenazas, usaré el texto de la OEA “Tendencias en la seguridad cibernética en América Latina y el Caribe y respuestas de los gobiernos”

El organismo encargado de la seguridad cibernética en Argentina es el Programa Nacional de Infraestructuras Críticas de información y Ciberseguridad (ICIC), que forma parte de la oficina Nacional de Tecnología de la Información (ONTI); que cuenta con un equipo de respuesta frente a

incidentes cibernéticos (CIRT). La Policía Federal de Argentina se encarga de la investigación de los delitos cibernéticos (Organización de los Estados Americanos, 2016, pág. 37).

En la actualidad algunas instituciones de educación argentinas brindan programas de certificación en materia de seguridad cibernética, incluyendo análisis forense digital[28]. El Instituto Nacional de Administración Pública (INAP) ofrece capacitación y cursos de ciberseguridad (Organización de los Estados Americanos, 2016, pág. 38).

El gobierno se prepara continuamente para estar en capacidad de responder ante las ciberamenazas emergentes; así, desde el año 2012 se han llevado a cabo Ejercicios Nacionales de Respuesta ante Incidentes Cibernéticos, que se realizan de forma anual (Organización de los Estados Americanos, 2016, pág. 38). También se llevan a cabo regularmente talleres sobre tecnologías cibernéticas emergentes, para garantizar la actualización de sus técnicos.

1.2.2.1.2. Brasil

Brasil es una economía de gran tamaño y que registró un fuerte ritmo de crecimiento entre el 2004 y el 2012; que forma parte del grupo denominado BRICS junto con otros cuatro grandes países emergentes, por lo que ha tenido que desarrollar capacidades avanzadas en cuanto a ciberseguridad y disuasión de ciberdelitos. La policía federal es la encargada de investigar todos los delitos que se registren en el país; esto incluye a los delitos cibernéticos. La policía también cuenta con un grupo especializado en la lucha contra la pornografía infantil en internet. En este sentido, únicamente si se cree que el delito cibernético lo requiere, se permite la intervención de personal de otras

[28] Análisis Forense Digital: De manera más formal podemos definir el Análisis Forense Digital como un conjunto de principios y técnicas que comprende el proceso de adquisición, conservación, documentación, análisis y presentación de evidencias digitales y que llegado el caso puedan ser aceptadas legalmente en un proceso judicial. (Delgado M. L., 2007, pág. 5)

unidades de la policía federal, o de otras instituciones. (Organización de los Estados Americanos, 2014, pág. 43)

El gobierno brasileño ha enfocado sus esfuerzos en el desarrollo de campañas de concientización, para promover en sus ciudadanos el uso inteligente y responsable de internet. Otra iniciativa del gobierno ha sido incentivar la cooperación entre el sector público y el privado mediante la entrega oportuna de informes sobre incidentes cibernéticos (Organización de los Estados Americanos, 2014, pág. 43). De igual forma la policía federal ha firmado varios acuerdos con empresas privadas como Microsoft.

En el año 2010 el gobierno de Brasil creó otra institución relacionada con la ciberseguridad, el Departamento de Seguridad de la Información, que define el Libro Verde de Seguridad Cibernética de Brasil. Para el año 2012 las fuerzas armadas brasileñas comienzan a discutir las preocupaciones del país en cuanto a defensa cibernética, en su Libro Blanco de Defensa Nacional (OBSERVATORIO DE LA CIBERSEGURIDAD EN AMÉRICA LATINA Y EL CARIBE, 2016, pág. 60).

En la actualidad, Brasil posee un comando de defensa cibernética formal y una escuela nacional de defensa cibernética, además del Centro de Defensa Cibernética del Ejército. También tiene equipos de respuesta ante incidentes cibernéticos tanto públicos como privados (OBSERVATORIO DE LA CIBERSEGURIDAD EN AMÉRICA LATINA Y EL CARIBE, 2016, pág. 60).

1.2.2.1.3. Chile

Chile ha demostrado un alto grado de madurez organizacional, al establecer varios organismos que comparten responsabilidad en cuanto a temas de la ciberseguridad del país. Tanto el Ministerio del Interior y Seguridad Pública como la Secretaría General de la Presidencia y la Subsecretaría de Telecomunicaciones juegan un papel muy importante dentro de la seguridad

cibernética, ya que establecen la política de ciberseguridad a nivel gubernamental. La policía nacional se encarga de investigar y perseguir de los delitos cibernéticos (Organización de los Estados Americanos, 2014, pág. 44).

Las diferentes ramas de las fuerzas armadas chilenas comparten responsabilidad en ciberdefensa y protección de información sensible, pero no operan mediante una estructura de mando central, que garantice la acción conjunta y los resultados deseados (OBSERVATORIO DE LA CIBERSEGURIDAD EN AMÉRICA LATINA Y EL CARIBE, 2016, pág. 62).

Sin embargo Chile, en lugar de centrarse en el fortalecimiento de un solo equipo de respuesta ante incidentes cibernéticos, el cual funciona desde el 2004, ha dirigido sus esfuerzos hacia el desarrollo de procedimientos y mejores prácticas de gestión de incidentes y seguridad cibernética, en general. Estos procedimientos fueron establecidos en el Decreto Supremo Número 1299 (Organización de los Estados Americanos, 2014, págs. 44-45).

En este cuerpo normativo, Chile ha establecido un marco jurídico para hacer frente a los ciberdelitos, ya que establece normas e introduce a los delitos cibernéticos en el Código Penal (OBSERVATORIO DE LA CIBERSEGURIDAD EN AMÉRICA LATINA Y EL CARIBE, 2016, pág. 62). En consecuencia Chile da pasos firmes para la construcción de leyes que contrarresten esta forma contemporánea de violencia virtual y para manejar los conflictos que se presenten.

1.2.2.1.4. Colombia

La ciberseguridad en Colombia se encuentra regida por el documento CONPES3701, que establece una política nacional de ciberseguridad y defensa; esta política define los roles, las responsabilidades y los campos de intervención del gobierno. En este marco fue creado el Centro Cibernético Policial, que investiga los delitos cibernéticos en todo el país, poniendo

especial atención a los grupos ilegales armados de Colombia, a las bandas criminales y al narcodelito (Organización de los Estados Americanos, 2014, pág. 46).

Complementariamente la Policía Nacional ha desarrollado sistemas internos de gestión de seguridad de la información y mantiene su propio equipo de respuesta ante incidentes cibernéticos (Organización de los Estados Americanos, 2014, pág. 46).

Para impulsar y gestionar el intercambio de información entre el sector privado y el sector público, se dictó el Decreto 1704, que establece los requisitos que deben cumplir los proveedores de redes y servicio de telecomunicaciones (Organización de los Estados Americanos, 2014, pág. 47).

Uno de los puntos fuertes de Colombia, en el tema de ciberseguridad, es su manejo de la cooperación internacional, ya que colaboran con varios organismos de la región, como la UNASUR, para combatir y responder ante ataques cibernéticos, según el informe de la OEA del año 2014.

A nivel regional vemos que los países sudamericanos basan sus respuestas en la concientización del uso inteligente del internet, la creación de instituciones destinadas a la protección de información y estructuras críticas del Estado, la capacitación del personal para que pueda responder ante los ciberataques y también usan la disuasión como herramienta de ciberdefensa. Esto quiere decir que en Sudamérica no se le ha puesto mayor énfasis al tema educativo y de prevención de ciberataques.

1.2.2.2. Respuestas Multilaterales a nivel regional

Dentro de las respuestas multilaterales, veremos las respuestas de la UNASUR y de la OEA, ya que son las organizaciones, dentro de la región, que más han tratado el tema de ciberseguridad, y que cuentan con iniciativas

que promueven la cooperación para conseguir una seguridad cibernética regional.

1.2.2.2.1. Unión de Naciones Suramericanas (UNASUR)

UNASUR ha declarado que es necesario construir un anillo de fibra óptica suramericano para que la región pueda estar conectada sin tener que depender de los Estados Unidos (Ramos, 2014, pág. 5). En consecuencia, cada año se incentiva la definición de un plan de acción que tendrá como objetivos principales el desarrollo de políticas de defensa, cooperación militar, acciones humanitarias y operaciones de paz. En base a esto, en el año 2012 se aprobó el Plan de Acción anual, que plantea la conformación de un grupo de trabajo que analice la factibilidad de implementar normas y mecanismos regionales en materia de ciberseguridad (Justribó, 2014, págs. 3-4).

En el 2013 la ciberdefensa tuvo mayor relevancia en la agende regional, luego de que se dieran a conocer las acciones de espionaje que realizó Estados Unidos sobre el gobierno brasileño.

En el 2014 el Consejo de Defensa Suramericano recomendó 4 puntos fundamentales que debían desarrollarse en lo que respecta la ciberseguridad de la región:

- La creación de un foro regional para intercambiar conocimientos, experiencias y procedimientos de ciberseguridad.
- Establecer una red de autoridades capacitadas para intercambiar información y mantener una colaboración constante en este ámbito.
- Definir la plataforma y procedimientos de comunicaciones que se aplicaran en la red de contactos.
- Profundizar la reflexión sobre los conceptos de ciberdefensa y ciberseguridad (Justribó, 2014, pág. 5).

Estas iniciativas han llevado a que los países busquen definir respuestas bilaterales frente a las ciberamenazas y la cooperación entre los países de la región. Como ejemplo podemos mencionar a la cooperación entre Argentina y Brasil, que se inició con el intercambio académico y la capacitación de sus militares en materia de ciberdefensa (Bustamante, Rivera, & Salinas, 2017)

1.2.2.2.2. Organización de Estados Americanos (OEA)

La OEA ha basado su estrategia de ciberseguridad en tres entidades fundamentales que son: el Comité Interamericano contra el Terrorismo (CICTE), la Comisión Interamericana de Telecomunicaciones (CITEL) y la REJMA. La CICTE tiene como objetivo la construcción de una red de vigilancia, alerta y aviso interamericana, para generar una respuesta oportuna y efectiva ante los incidentes informáticos. La CITEL se encarga de la identificación e implementación de normas técnicas para la construcción de una estructura informática segura. La REJMA establece y maneja las herramientas legales para proteger a los usuarios de redes de información y de internet (Morán, 2015, pág. 07).

También promueve la creación de un CERT en cada uno de los Estados miembro, y publica periódicamente informes que exponen las principales tendencias sobre la gestión de la ciberseguridad de Latinoamérica y se describe la implementación y la evolución de las medidas de frente a la ciberseguridad establecidos por parte de los Estados miembros (Morán, 2015, pág. 07).

El portal de cooperación en delitos cibernéticos de la OEA es fundamental también para su estrategia de seguridad cibernética ya que facilita la cooperación y el intercambio de información entre los países miembro, de modo que la persecución e investigación de estos delitos sea más efectiva (Departamento de Cooperación Jurídica de la OEA, 2017)

A nivel regional podemos observar que las organizaciones buscan generar una ciberseguridad homogénea dentro de la región, es decir que quiere reunir y desarrollar las capacidades de sus miembros mediante la cooperación internacional para hacerle frente a las ciberamenazas y a los ciberataques como un solo bloque; ello implica consensuar definiciones compatibles, normas comunes y protocolos universalmente aplicados. Para alcanzar esto, también han creado instituciones especializadas y han generado iniciativas que fomentan la cooperación internacional y la concientización sobre los riesgos del ciberespacio.

CAPITULO 2

2. EL ESTADO ECUATORIANO FRENTE A LA CIBERDEFENSA: PERIODO 2008-2015

En el artículo 393 de la Constitución de la República dictado en el 2008, se estipula que: “El Estado garantizará la seguridad humana a través de políticas y acciones integradas, para asegurar la convivencia pacífica de las personas, promover una cultura de paz y prevenir las formas de violencia y discriminación y la comisión de infracciones y delitos. La planificación y aplicación de estas políticas es responsabilidad de los organismos especializados en los diferentes niveles de gobierno.” (MINISTERIO DE DEFENSA NACIONAL, 2014, pág. 2)

En este capítulo se expondrán los antecedentes fundamentales de la comprensión e identificación de las ciberamenazas en el caso del Ecuador y se analizarán las estrategias de ciberdefensa que ha mantenido el Estado ecuatoriano en el periodo 2008-2015. Para este análisis se revisarán los antecedentes fundamentales de las ciberamenazas en el país, las capacidades de las instituciones públicas destinadas a precautelar la ciberseguridad ecuatoriana, las respuestas que ha generado el Estado durante este periodo frente a las ciberamenazas, y finalmente la legislación que maneja el Estado frente a los delitos cibernéticos.

2.1. Antecedentes fundamentales de la ciberseguridad en el Ecuador

En el año 2008, se registraba que solamente 7% de los hogares ecuatorianos tenían acceso a internet (INEC, 2008). En el 2015 vemos que los hogares que tienen acceso al internet en el Ecuador llegan al 32,8% (INEC, 2015). Este incremento se ve reflejado en el hecho de que las entidades financieras y comerciales, públicas y privadas, han implementado nuevos software para automatizar su manejo y han creado páginas web para ofrecer sus servicios en línea. En cuanto a líneas móviles activas de teléfonos con acceso a internet, en el

2013 llegaron a los 17 millones, y la cantidad de parroquias que no contaban con cobertura 3G y 3.5G fue del 32%. (Delgado A. , 2014)

En el 2014 el Ecuador estuvo posicionado en el puesto 82 dentro del ranking global de los países que más utilizan las TICs buscando una transformación productiva, desarrollo económico y bienestar social (Foro Económico Mundial, 2017). La creciente adopción de las TICs ha significado un aporte no cuantificado al desarrollo del país; sin embargo también ha generado el aumento problemas de ciberseguridad para el Estado, sus entidades, las empresas públicas y privadas, al igual que para todos sus ciudadanos.

Pese a que existe una brecha informática entre las zonas rurales y las zonas urbanas del país, el Estado ha trabajado en las zonas rurales para mejorar su conectividad a internet mediante programas de equipamiento y conexión que ha llevado a cabo el Ministerio de Comunicaciones. Uno de los proyectos son los centros comunitarios Infocentros que se comenzaron a instalar en el año 2012, ellos han provisto de computadoras a 7541 estudiantes en todo el país y de acceso a internet a 491 comunidades (Freedom House, 2016).

Desde 2010 las entidades diplomáticas, militares y gubernamentales ecuatorianas han sido víctimas de ciberespionaje, pero es en el 2011 donde comienzan a generarse ataques cibernéticos considerables. En este año, Kaspersky Lab[29] informó que, según sus datos, el delito cibernético que más ocurrió en el país fue el fraude bancario, por lo cual se calcula que el país perdió 5 millones de dólares (EL COMERCIO, 2017).

También se registró un ciberataque a las páginas web del gobierno ecuatoriano, el cual las dejó sin servicio durante dos horas (EL UNIVERSO, 2011), y también existió una filtración de información de las identidades de miembros de la policía nacional, de trabajadores del aeropuerto de Quito e información de CNT por parte

[29] "Kaspersky Lab es una compañía global de ciberseguridad que proporciona soluciones y servicios de seguridad para proteger a las empresas, la infraestructura crítica, los gobiernos y los consumidores de todo el mundo." (Kaspersky Lab, 2017)

de Anonymous, como rechazo a la falta de libertad de expresión (International Business Times, 2017). Según la fiscalía nacional, el 2012 los delitos informáticos perjudicaron a 885 usuarios del sistema financiero, de modo que las denuncias aumentaron 163,88% más que en el 2010 (EL UNIVERSO, 2012). Al siguiente año se realizaron 1400 ataques cibernéticos al sistema electoral, intentando sabotearlo durante las nuevas elecciones presidenciales; uno de los ataques se realizó desde un centro tecnológico ubicado en un país de primer mundo, el cual no ha sido revelado (Rogers, 2013).

En Julio del 2013, un hacker autodenominado el Bufón atacó la bolsa de valores ecuatoriana como retaliación por mantener asilado a Julian Assange y analizar la idea de otorgar asilo a Edward Snowden, porque considera que los dos son unos traidores y que han puesto en riesgo las vidas de los estadounidenses (LIEBELSON, 2013).

Este ataque nos deja ver que el hecho de haber brindado asilo a un hacker como Julián Assange nos ha convertido en blanco para ataques cibernéticos y nos han puesto en una disyuntiva dentro de la lucha contra el ciberespionaje, puesto que estamos protegiendo a una persona que es perseguida por este delito informático.

Kaspersky anuncio que en el 2014 el Ecuador ocupó el octavo lugar entre los países más atacados cibernéticamente en la región[30]. A nivel mundial el ecuador tuvo un 42,33% de infecciones por virus informáticos (Panda Lab, 2017). En el mismo año, el gobierno ecuatoriano acusó a Chevron[31] de haber obtenido de forma ilícita, conversaciones confidenciales del presidente y de otros funcionarios del Estado (Morrison, 2014). El presidente Correa denuncio que sufrió ataques cibernéticos que se realizaron, presuntamente, desde los Estados Unidos, ante lo cual se anunció la creación de un comando de ciberseguridad que resguardaría la información confidencial del Estado y sus infraestructuras críticas.

[30] "En el documento se informa que el 24,6% de usuarios de internet han sido víctimas de intentos de infección." (ÚLTIMA HORA, 2016)

[31] Empresa petrolera estadounidense que compró el en 2001 a la empresa TEXACO, la cual extrajo millones de barriles de petróleo en el Ecuador sin un mecanismo adecuado, por lo cual hoy posee una demanda por parte del país. (Ministerio de Relaciones Exteriores y Movilidad Humana, 2017)

Para el 2015 los ataques cibernéticos que recibió el Ecuador se tornaron más sofisticados. Una banda de ciberdelincuentes atacó al sistema de contratación pública, buscando beneficiar a determinadas empresas y microempresas para obtener contratos en el sector público (Bravo, 2015). Fueron atacadas 17 empresas ecuatorianas por cibermáfias pero no hubo una respuesta eficaz que detuviera el virus (EL COMERCIO, 2015).

El grupo Lazarus atacó al Banco del Austro, del cual se robaron 12 millones de dólares que fueron transfirieron a una cuenta bancaria en Estados Unidos. Esto alertó de sobremanera al gobierno ecuatoriano ya que se detectaron graves falencias y vulnerabilidades dentro de sus páginas web y las de empresas privada.

La vulnerabilidad que presenta el Ecuador ante los ciberataques se volvió a manifestar en el mismo año cuando un virus infectó durante cinco días a computadores de empresas privadas en Quito, Guayaquil y Cuenca; en el ataque se encriptaron[32] documentos con información sensible de las empresas y una de las empresas afectadas perdió carpetas en las que almacenaba datos del departamento de contabilidad (Ortega, 2015). De modo que el Ecuador fue víctima de un ciberataque masivo, cosa que hasta el 2014 no había ocurrido. Esto denota la sofisticación y el desarrollo que han tenido los ataques cibernéticos desde el año 2008 hasta el año 2015. El avance que han tenido los malware a nivel mundial no es ajeno a la realidad ecuatoriana, ya que depende de sistemas informáticos para desarrollarse.

2.2. Estrategia de Ciberdefensa Nacional del Ecuador

2.2.1. Instituciones destinadas a la Ciberseguridad

[32] Encriptar: "Ocultar datos mediante una clave para que no puedan ser interpretados por los que no la tienen este sistema permite encriptar datos personales o financieros". (The Free Dictionary, 2017)

Uno de los principales organismos estatales encargado de regular y gestionar las TICs en el Ecuador es la Superintendencia de Telecomunicaciones (SUPERTEL), que fue creada en 1992, la cual se encarga principalmente de velar por el respeto a los derechos de los usuarios de las Tecnologías de Información y Comunicación, la innovación de mecanismos, procedimientos y sistemas de control, de promover el desarrollo de las telecomunicaciones, y de vigilar que los prestadores privados de servicios de telecomunicaciones sean efectivos y satisfagan las necesidades del usuario (SUPERTEL, 2016).

La ciberseguridad es primordial para la SUPERTEL y para garantizarla, en el 2014 se creó un equipo de respuesta frente a Incidentes informáticos, denominado EcuCERT[33]. Este equipo logró acreditación internacional gracias a su nivel técnico, lo cual le autoriza para gestionar incidentes de seguridad informática en Ecuador y poder planificar acciones de respuesta a los ciberataques conjuntamente con CERTs internacionales.

De acuerdo a la rendición de cuentas de la Superintendecia de Telecomunicaciones del 2014, EcuCERT también es parte del "Forum of Incident Reponse and Security Teams" (FIRST)[34]. El EcuCERT astá conformado por un equipo de expertos que tienen la labor de llevar a cabo y coordinan las acciones de respuesta ante una amenaza cibernética; también de gestionar las denuncias de ciberincidentes y asesorar en temas de ciberseguridad a las víctimas de ataques.

El Equipo de Respuesta a Incidentes Informáticos del Ecuador tiene como potestad tratar incidentes de seguridad informáticos, tanto nacionales como internacionales y emitir avisos en caso de riesgos informáticos; se encarga de la

[33] "EcuCert es el Centro de Respuesta a Incidentes Informáticos de la Agencia de Regulación y Control de las Telecomunicaciones del Ecuador. Tiene como objetivo contribuir con la seguridad de las redes de telecomunicaciones de todo el país, así como también con la seguridad del uso de la red de internet." (EcuCERT, 2017)

[34] "FIRST: La mayor red de equipos de seguridad del mundo" (SUPERTEL, 2016). "FIRST reúne una amplia variedad de equipos de seguridad y de respuesta a incidentes, incluyendo especialmente equipos de seguridad de productos de los sectores gubernamental, comercial y académico." (FIRST, 2017)

investigación de vulnerabilidades en los sistemas estatales y privados, cuenta con un laboratorio forense para analizar los incidentes y tiene como funciones también desarrollar aplicaciones, realizar capacitaciones y organizar campañas de sensibilización en materia de seguridad informática (SUPERTEL, 2016).

El Ministerio de Defensa, como institución creada para defender la soberanía, la integridad territorial y proteger las libertades, derechos y garantías de los ciudadanos, debe desempeñar las mismas tareas en el ciberespacio, por lo que en septiembre del 2014 se crea el Sistema de Ciberdefensa del Ministerio de Defensa Nacional que articula estrategias política y militares para implementar normativas y coordinar acciones de ciberdefensa.

(Ministerio de Defensa Nacional, 2014, pág. 4)

Dentro del sistema de ciberdefensa se encuentra el Comité de Ciberdefensa[35], encargado de articular a los diferentes organismos internos para prevenir,

[35] Al que se le asignan las siguientes funciones, en:

- "Diseñar la concepción político-estratégica de Ciberdefensa en concordancia con la Agenda Política de la Defensa."

detectar y defender al país ante amenazas cibernéticas, también está el Comité de Tecnologías de la Información y Comunicación de la Defensa (COTICDE)[36], que se responsabiliza de asesorar al Comité de Ciberdefensa y de revisar el esquema gubernamental de seguridad de la información del presidente. (Ministerio de Defensa Nacional, 2014)

Con la firma del acuerdo 281, el 24 de septiembre del 2014, el Ministerio de Defensa crea el Comando de Ciberdefensa, considerado un comando de las Fuerzas Armadas[37], conformado por personal técnico civil y militar; para defender y proteger las infraestructuras críticas y la información confidencial del Estado (Ministerio de Defensa Nacional, 2014), por medio de operaciones de protección y acciones de disuasión, prevención y reacción ante un ataque (Borbúa, Herrera, & Reyes, 2017, pág. 38).

- "Monitorear y evaluar la implementación de las políticas de Ciberdefensa, así como del adecuado funcionamiento de los sistemas de información, comunicación e inteligencia relativos al ciberespacio."
- "Promover la concepción política estratégica de Ciberdefensa a nivel nacional."
- "Coordinar con las instancias correspondientes, el diseño de políticas públicas a nivel nacional en el ámbito de su competencia."
- "Promover iniciativas de capacitación y formación en el ámbito de ciberdefensa."
  (MINISTERIO DE DEFENSA NACIONAL, 2014)

[36] Las competencias del COTICDE son:

- "Coordinar con el Comando de Ciberdefensa Conjunto las estrategias necesarias para la ejecución del Plan de Ciberdefensa."
- "Articular el adecuado funcionamiento de los sistemas de información, comunicación e inteligencia relativos a la Ciberdefensa, y evaluarlo periódicamente."
- "Proponer disposiciones y directrices para el desarrollo e implementación de la capacidad de "Ciberdefensa, a ser concertadas en el Comité de Ciberdefensa."
- "Promover la política de Ciberdefensa a nivel nacional y regional."
  (MINISTERIO DE DEFENSA NACIONAL, 2014)

[37] Sus funciones son:

- "Proteger la infraestructura crítica del Estado en el corto, mediano y largo plazo."
- "Desarrollar la capacidad de Ciberdefensa en: exploración, prevención, defensa y respuesta."
- "Generar una estructura del Comando de acuerdo al modelo de gestión por procesos de la Defensa."
- "Elaborar el Plan de Ciberdefensa con conocimiento y análisis del Comité de Ciberdefensa y aprobación de la máxima autoridad del Ministerio de Defensa."
- "Coordinar con la Dirección de Ciberdefensa los temas de su competencia."
  (MINISTERIO DE DEFENSA NACIONAL, 2014)

Estructura Organizacional del Comando de Ciberdefensa

(Comando Conjunto de las Fuerzas Armadas y Comando de Ciberdefensa)

El Comando de Ciberdefensa a pesar de estar conformado por ingenieros en sistemas, ingenieros electrónicos, masters en seguridad informática y de sistemas, capacitados con cursos como Ethical Hacking, Linux e Informática Forense (Jefe de Estado Mayor del Comando de Ciberseguridad, 2017), presenta debilidades en cuanto a capacitación de sus miembros e infraestructura y dado a que su creación es relativamente reciente, no cuenta con la capacidad para detener un ataque cibernético (Peralvo, 2015, págs. 26-27), ni con la capacidad de proteger la infraestructura crítica digital del Estado, ya que hasta el 2015 estaban recién generando su infraestructura informática y se aspira que para el 2021 se consigan las capacidades necesarias para brindar una seguridad informática óptima. (Jefe de Estado Mayor del Comando de Ciberseguridad, 2017)

La Policía Nacional también desempeña un rol dentro de la ciberseguridad nacional; esta institución incluye a la Unidad de Investigación del Cibercrimen la cual coopera con la INTERPOL para promover el intercambio de información con el sector privado y elaborar de un programa de capacitación en cuanto a

evidencia digital para el personal de los tribunales, miembros de la policía e investigadores (OEA ; BID, 2016).

La Secretaría de Inteligencia (SENAIN) se encarga de la producción inteligencia y contrainteligencia para garantizar una seguridad integral del Estado ecuatoriano y des Buen Vivir. Dentro del ámbito de ciberseguridad, busca incrementar los mecanismos de seguridad cibernéticas para precautelar los sistemas de comunicación estratégica del Estado y la información sensible, en base a la promoción de políticas públicas y al desarrollo de aplicaciones web que contribuyan con la seguridad integral. También pretende ser proveedor de sistemas de alerta temprana ante amenazas y riesgos tecnológicos. (Secretaría de Inteligencia, 2017)

La Secretaría Nacional de la Administración Pública (SNAP) fomenta la implementación de una plataforma de gobernanza electrónica, supervisa la gestión de la seguridad de la información mediante decretos y acuerdos establecidos a nivel ministerial. La SNAP junto a la Secretaría Nacional y el Ministerio de Telecomunicaciones y de la Sociedad de la información, formaron la Comisión para la Seguridad Informática, con el fin de establecer normas de seguridad informática, proteger la infraestructura computacional y proteger información confidencial de las entidades públicas (Delgado A. , 2014).

Evolución de Ecuador en ranking de e-government o gobierno electrónico (EGDI)

Indicador	2008	2010	2012
Servicios en Línea	0,4448	0,3175	0,4575
Capital Humano	0,8566	0,8230	0,7549
Infraestructura	0,1472	0,1657	0,2482
Participación por medios electrónicos	0,1136	0,1571	0,2368
Puesto en el ranking	75	97	102

(Secretaría Nacional de la Administración Públlica, 2017, pág. 21)

El retroceso, que vemos en el gráfico, que ha tenido el Ecuador en materia de gobierno electrónico se debe a que no se ha logrado generar un esfuerzo homogéneo para su desarrollo, lo cual ha hecho que aunque el país haya tenido avances, otros países lo superen en el ranking ya que avanzan con mayor rapidez (Secretaría Nacional de la Administración Públlica, 2017, pág. 21).

Este es el desglose presupuestario que presentó la SNAP para el gobierno electrónico entre el 2014 y el 2015.

PILAR	PRESUPUESTO	PESO
Marco regulatorio	$ 10.520.452,80	2,5%
Personas	$ 64.646.122,00	15,3%
Servicios y procesos	$ 207.431.817,97	49,2%
Tecnologías de la Información y Comunicaciones	$ 139.270.811,89	33,0%
TOTAL	$ 421.869.204,66	100,0%

(Secretaría Nacional de la Administración Públlica, 2017, pág. 43)

Este presupuesto asignado por el gobierno ayudó a que el Ecuador para el 2015 escale en el ranking mundial y obtenga un nivel alto de gobernanza electrónica; sin embargo sigue debajo de países de la región como Colombia, Argentina, Brasil y Chile (Naciones Unidas, 2016, pág. 155).

2.2.2. Otras respuestas del Estado Ecuatoriano ante las ciberamenazas y participación en instancias multilaterales

Desde aproximadamente el 2010, el Estado ecuatoriano ha planteado su preocupación por hacer frente a las nuevas amenazas que representa el ciberespacio; y parece comprender que el espacio cibernético es vital para la supervivencia del Estado y la seguridad de sus ciudadanos. En tal sentido el gobierno ha tomado decisiones políticas y ha iniciado proyectos para minimizar los problemas de ciberseguridad.

A partir del 2012 se inició el proyecto de EcuCERT con el fin de gestionar incidentes informáticos, este fue implementado en el 2014 (OEA ; BID, 2016, pág. 70). La creación e implementación del EcuCert[38] fue un paso importante para el Ecuador en materia de ciberseguridad ya que supone no solo un adecuado tratamiento de las denuncias de ataques cibernéticos, sino también la cooperación internacional en la lucha contra las ciberamenazas. (Romero, Ronquillo, Tituaña, & Aranda, 2011, pág. 4)

En el 2013, debido a las declaraciones de Snowden acerca del espionaje masivo que realizaba Estados Unidos, el Ministerio de Coordinación de Seguridad del Ecuador informó que se implementarían procesos de seguridad para combatir el ciberespionaje a altos funcionarios del Estado (Delgado A. , 2014).

Uno de los procesos que se implementaría era el cifrado de los documentos para mantener a salvo información confidencial que posean los altos funcionarios acerca se las infraestructuras criticas del Estado. También se conformó el Centro de Operaciones Estratégico Tecnológico que llevó a cabo un monitoreo de ataques informáticos a equipos de algunas instituciones públicas (OEA ; BID, 2016, pág. 70).

El gobierno ecuatoriano ha designado a la Secretaría Nacional de la Administración Pública como el encargado de proveer una plataforma de gobierno electrónico; por lo que estableció el 25 de septiembre del 2013, el Esquema Gubernamental de Seguridad de la Información, o también conocido como acuerdo 166. La secretaría justificó la elaboración de este esquema considerando que las TICs son fundamentales para el desarrollo y desempeño de las instituciones públicas y privadas, lo que supone un alto riesgo de espionaje

[38] "El EcuCERT tiene como propósito establecer criterios generales y específicos en materia de ciberseguridad para garantizar la seguridad de los servicios de telecomunicaciones, la información transmitida y la invulnerabilidad de la red mediante la gestión, conjunta con los prestadores de servicios de telecomunicaciones del país, de vulnerabilidades e incidentes de seguridad informática. Controlar que dichos prestadores de servicios adopten medidas de seguridad y un equipamiento adecuado a las necesidades del usuario. También realiza actividades de capacitación, educación y entrenamiento sobre el buen uso de las tecnologías y coopera internacionalmente para que se creen otros CERTs." (EcuCERT, 2017)

global, sabotajes a infraestructuras críticas y la suplantación de identidad, factores que ponen en peligro tanto los derechos de los ciudadanos como a la seguridad del Estado. Dentro del acuerdo se manifestó lo siguiente:

> "Es importante adoptar políticas, estrategias, normas, procesos, procedimientos, tecnologías y medios necesarios para mantener la seguridad en la información que se genera y custodia en diferentes medios y formatos de las entidades de la Administración Pública Central, Institucional y que dependen de la Función Ejecutiva." (Secretaría Nacional de la Administración Pública, 2013, pág. 1)

> "La Administración Pública de forma integral y coordinada debe propender a minimizar o anular riesgos en la información así como proteger la infraestructura gubernamental, más aún si es estratégica, de los denominados ataques informáticos o cibernéticos." (Secretaría Nacional de la Administración Pública, 2013, pág. 1)

A pesar de que la Secretaría de Administración Pública obligara a las empresas públicas a adoptar este esquema gubernamental, no todas lo han implementado, generando vacíos y ahondando las vulnerabilidades de la seguridad cibernética nacional (Borbúa, Herrera, & Reyes, 2017, pág. 37).

No es suficiente con implantar normas, política y procesos de ciberseguridad para garantizar la seguridad del Estado y de sus ciudadanos; debe colocarse en el inconsciente colectivo la necesidad de prevención ante las ciberamenazas, por lo que la Secretaría de Inteligencia propuso una campaña para promover una cultura de seguridad informática (OEA ; BID, 2016), la implementación de carreras especializadas en ciberseguridad y la dotación de cursos al personal de empresas públicas y privadas, que se les instruya acerca de lo que son las ciberamenazas y los procesos de prevención.

En el mes de mayo del 2014 se planteó la inclusión de la ciberseguridad en el pensum académico de la las instituciones de formación militar (Delgado A. , 2014), lo cual ratifica la importancia que se asigna a la seguridad cibernética y supone la investigación a fondo de las ciberamenazas, las vulnerabilidades de los sistemas informáticos, la creación de software que prevenga y contrarreste los ataques, y su implementación, lo que abre un abanico de posibilidades para el desarrollo de la ciberseguridad en el Ecuador.

El Ministerio de Defensa creó el Comando de Operaciones de Ciberdefensa como parte de las Fuerzas Armadas, con el fin de proteger al Estado ante cualquier ataque cibernético; para ello se destinaron 8 millones de dólares que sirvieron para arrancar el proyecto (EL UNIVERSO, 2014).

El Ministerio también ha buscado cooperación tecnológica y capacitación militar con China (La República, 2014), de forma que se aumentaron las plazas para que personal activo militar vaya a seguir cursos en el país asiático y se instruyan en cuanto a modelos nuevos de ciberseguridad. El Comando de Ciberdefensa fue implementado en el 2015 y ya se han capacitado a varios militares en academias e institutos militares de China.

MATRIZ DE LA PROGRAMACION ANUAL DE PLANIFICACION DE INVERSION DE LA DEFENSA 2015

NOMBRE DEL PROYECTO	PRESUPUESTO CODIFICADO 31 MAYO 2015
AMPLIACIÓN DE LA INFRAESTRUCTURA DE TRANSPORTE LIVIANO PARA LA FUERZA TERRESTRE (HELICOPTEROS LIVIANOS MULTIPROPOSITO).	4.617.498,08
RECUPERACION DE LA CAPACIDAD OPERATIVA DE LA FUERZA DE REACCION INMEDIATA DEL SISTEMA DE DEFENSA AÉREA NACIONAL (FAE).	5.464.715,40
MODERNIZACIÓN DE UNIDADES SUBMARINAS	6.930.407,07
RECUPERACION DE LA MOVILIDAD DE LAS CORBETAS LOS RIOS, MANABI Y LOJA	20.000.000,00
IMPLEMENTACION DE LA CAPACIDAD DE CIBERDEFENSA EN FF AA	5.131.456,00

(Ministerio de Defensa Nacional, 2016)

La Policía Nacional por su lado también ha llevado a cabo acciones para hacer frente a las ciberamenazas; ha realizado una campaña interna de concientización acerca de las ciberamenazas y del manejo de la información confidencial de la institución, de las redes sociales y de los sistemas tecnológicos, de tal forma que todo su personal pueda llevar esta información a sus hogares y se genere una "cadena de conocimiento". También adoptaron las políticas estipuladas en el acuerdo 166 (Cpnt. Toapanta, 2015). Elementos de la institución también han dictado conferencias sobre ciberseguridad en escuelas y colegios, recomendando normas de seguridad a la hora de utilizar un dispositivo electrónico.

El gobierno también ha participado en acciones multilaterales surgidas ante la problemática de la ciberdefensa, por ejemplo para apoyar la iniciativa que propicia el intercambio de información con la Escuela Sudamericana de Defensa y generar proyectos multilaterales de ciberdefensa y una visión regional compartida con respecto a la defensa cibernética en el marco de la UNASUR.

Ecuador mantiene cooperación sobre temas de seguridad cibernética con otros países, en su calidad de miembro de las siguientes organizaciones:

- UNASUR que busca una visión unificada de la ciberdefensa en la región.

- OEA que propicia iniciativas para que sus Estados miembros puedan desarrollar de la mejor manera sus capacidades de defensa cibernética.

- ITU-IMPACT, que es el brazo ejecutor de la ciberseguridad de la Unión Internacional de Comunicaciones y es el encargado de brindar asistencia y apoyo de seguridad cibernética a los Estados miembros (IMPACT, 2017).

- LACNIC, uno de los 5 registros regionales de direcciones de internet en el mundo, que impulsa políticas de cooperación regional, para contribuir al objetivo de lograr una conectividad efectiva y segura a internet dentro de la comunidad regional (LACNIC, 2017).

- FIRST, confederación internacional de equipos de respuesta a incidentes, que busca manejar de forma cooperativa la gestión de incidentes de ciberseguridad y promover programas de prevención de ataques (FIRST, 2017).

- El Instituto de Ingeniería de Software (SEI) del CERT, que estudia y resuelve problemas de ciberseguridad, desarrolla sistemas de red e investiga las vulnerabilidades de productos de software (CERT, 2016).

A pesar de todas las respuestas que hemos detallado anteriormente, el Estado ecuatoriano no ha realizado hasta hora un registro de cuáles son las infraestructuras críticas a proteger ni se ha definido la información estratégica en el ámbito público como en el privado, por lo que cada institución encargada de la ciberseguridad ha manejado este tema a discreción y han tomado iniciativas basadas en los intereses y necesidades de cada una de ellas. En consecuencia, hace que las acciones de ciberdefensa sean predominantemente fragmentadas y poco efectivas, generando más vulnerabilidades y una ciberseguridad nacional limitada.

2.2.3. Legislación y Políticas de Ciberseguridad

La Constitución de la República del Ecuador, dentro del título II, capitulo segundo, sección tercera, establece que todas las personas tienen derecho al acceso universal a las tecnologías de información y comunicación. En el título VII, capitulo primero, sección novena, que trata de la gestión de riesgo, el Estado se compromete a proteger a las personas, entidades públicas y entidades privadas frente a amenazas existentes y potenciales, ya sea internas o externas, que afecten al territorio ecuatoriano, fortalecer las capacidades de los ciudadanos y de sus empresas para combatir y prevenir los riesgos, y finalmente coordinar acciones para reducir las vulnerabilidades (Asamblea Constituyente, 2008). Esto quiere decir que el Estado está en la obligación de proteger a las empresas

públicas y a sus ciudadanos frente a las amenazas cibernéticas, ya que al tener acceso universal a las TICs, se encuentran vulnerables frente a cualquier ciberataque.

En agosto del 2014 se puso en vigencia el Código Orgánico Integral Penal (COIP), que establece sanciones para los delitos informáticos. En caso de obtención y mal manejo de información confidencial[39] establece sanciones de tres a cinco años de prisión y la pena es de siete a diez años si se la divulga; el ciberespionaje[40] es sancionado de siete y diez años de prisión. (Asamblea Nacional, 2014)

El acercamiento con fines sexuales a menores de dieciocho años por medios informáticos es sancionado con privación de libertad de uno a tres años[41]y la oferta de servicios sexuales con menores en el internet está sancionada con penas de siete a diez años de prisión[42]. La revelación ilegal de bases de datos también es sancionada con entre uno y tres años de prisión. Estos son los

[39] "Artículo 233.- La o el servidor público que, utilizando cualquier medio electrónico o informático, obtenga este tipo de información, será sancionado con pena privativa de libertad de tres a cinco años. Cuando se trate de información reservada, cuya revelación pueda comprometer gravemente la seguridad del Estado, la o el servidor público encargado de la custodia o utilización legítima de la información que sin la autorización correspondiente revele dicha información, será sancionado con pena privativa de libertad de siete a diez años y la inhabilitación para ejercer un cargo o función pública por seis meses, siempre que no se configure otra infracción de mayor gravedad." (Asamblea Nacional, 2014, pág. 5)

[40] "Artículo 354.- La o el servidor militar, policial o de servicios de inteligencia que en tiempo de paz realice uno de estos actos, será sancionado con pena privativa de libertad de siete a diez años, cuando: 1. Obtenga, difunda, falsee o inutilice información clasificada legalmente y que su uso o empleo por país extranjero atente contra la seguridad y la soberanía del Estado. 2. Intercepte, sustraiga, copie información, archivos, fotografías, filmaciones, grabaciones u otros sobre tropas, equipos, operaciones o misiones de carácter militar o policial. 3. Envíe documentos, informes, gráficos u objetos que pongan en riesgo la seguridad o la soberanía del Estado, sin estar obligado a hacerlo o al haber sido forzado no informe inmediatamente del hecho a las autoridades competentes. 4. Oculte información relevante a los mandos militares o policiales nacionales. 5. Altere, suprima, destruya, desvíe, incluso temporalmente, información u objetos de naturaleza militar relevantes para la seguridad, la soberanía o la integridad territorial." (Asamblea Nacional, 2014, pág. 131)

[41] "Artículo 173.- La persona que a través de un medio electrónico o telemático proponga concertar un encuentro con una persona menor de dieciocho años, siempre que tal propuesta se acompañe de actos materiales encaminados al acercamiento con finalidad sexual o erótica, será sancionada con pena privativa de libertad de uno a tres años." (Asamblea Nacional, 2014, pág. 78)

[42] "Artículo 174.- La persona, que utilice o facilite el correo electrónico, chat, mensajería instantánea, redes sociales, blogs, fotoblogs, juegos en red o cualquier otro medio electrónico o telemático para ofrecer servicios sexuales con menores de dieciocho años de edad, será sancionada con pena privativa de libertad de siete a diez años." (Asamblea Nacional, 2014, pág. 78)

artículos más relevantes que se encuentran dentro del Código Penal en materia de ciberseguridad.

El Código Penal, con los artículos antes mencionados garantiza la sanción ante los delitos cibernéticos, pero como ya hemos visto durante el desarrollo de esta tesis, las entidades llamadas a investigar todas las irregularidades cibernéticas no tienen la experiencia suficiente para llevar a cabo sus labores de manera efectiva, de modo que identificar a los autores de los ciberdelitos es un trabajo que el Estado no ha podido cristalizar completamente; sin embargo ha buscado el apoyo del sector privado para hacer reformas al Código de manera que se pueda afrontar a la delincuencia cibernética de manera adecuada.

La Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos del 2002, es otro de los marcos normativos definido por el Ecuador, que incluye normas sobre la ciberseguridad del país; por ejemplo condena y multa a toda persona que destruya de forma maliciosa documentos, programas, bases de datos o información vital para el Estado, o la empresa privada, también a las personas que alteren documentación con el fin de agraviar a un tercera y que viole la privacidad de otro mediante ciberespionaje (Congreso Nacional, 2016).

Por otro lado el Esquema Gubernamental de Seguridad de la Información (Acuerdo 166), creado el 25 de septiembre del 2013, que contempla políticas de ciberseguridad, entre las cuales se encuentran las siguientes:

- Políticas sobre la organización de la seguridad de la información, las cuales se basan en la conformación del Comité de Gestión de la Seguridad de la Información dentro de cada institución y la designación de sus integrantes; este comité deberá definir las normas de seguridad cibernética, monitorear nuevos riesgos e incidentes de seguridad y realizar controles específicos antes de implementar un nuevo sistema (Secretaría Nacional de la Administración Pública, 2013).

- Políticas de gestión de activos, que plantean el inventario de activos físicos (Hardware) y electrónicos (Software); la designación del personal responsable de los activos y el uso correcto de los activos (Secretaría Nacional de la Administración Pública, 2013).

- Políticas de Gestión de Comunicación y Operaciones que abarcan el manejo de la documentación, los procedimientos de operación, separación de las instancias de Desarrollo, Pruebas, Capacitación y Producción, y controles contra códigos maliciosos de un sistema nuevo. (Secretaría Nacional de la Administración Pública, 2013)

Este acuerdo fue adoptado en todas las instituciones estatales por disposición de la Secretaría Nacional de Administración Pública.

En la Agenda Política de Defensa también se incluyen las políticas que atañan a la ciberdefensa pero ellas están dirigidas específicamente a las responsabilidades de las Fuerzas Armadas. Dentro de la política para garantizar la soberanía e integridad territorial para la consecución del buen vivir en el marco de los derechos humanos se destaca el desarrollo de capacidades para la ciberdefensa. Otra política que contempla la agenda es la de proteger la información estratégica del Estado, en materia de defensa, que estipula la protección de infraestructura crítica, de redes estratégicas y de información confidencial, el fortalecimiento de mecanismos interinstitucionales para combatir las ciberamenazas y la participación en las iniciativas de la UNASUR en el ámbito de la ciberseguridad (Delgado, Garcés, & Dávila, 2014).

CONCLUSIONES

La información digital se ha convertido en parte vital de cualquier Estado ya que, las empresas públicas de cualquier país desarrollado o en vías de desarrollo han digitalizado casi en su totalidad la documentación estratégica y han automatizado sus procesos. Sus ciudadanos han hecho lo propio y también han digitalizado su información confidencial y realizan la mayoría de sus transacciones vía internet. Esto genera inseguridad tanto para el Estado como para sus ciudadanos, porque hackers, organizaciones, Estados y organizaciones terroristas tiene interés en determinada información y están dispuestos a utilizar cualquier herramienta de ciberataque para obtenerla. Lo que ha puesto a la ciberseguridad como un aspecto prioritario para el Estado.

Hemos visto a los largo de la investigación que la meta de una ciberseguridad optima es muy difícil de alcanzar debido a la naturaleza anárquica del ciberespacio. Países de primer mundo como China y Estados Unidos, que tienen una buena trayectoria trabajando en sus capacidades cibernéticas, no han podido conseguir una ciberseguridad integral y efectiva de forma individual que los blinde ante los ciberataques.

La cooperación internacional tampoco ha sido la solución efectiva que todos pensaríamos, ya que, como lo pudimos apreciar anteriormente, organizaciones como la ONU o la OTAN tampoco han podido conformar una ciberseguridad apropiada, con el agravante de que su meta es alcanzar una gobernanza electrónica mundial, lo cual es casi imposible en vista de que cada país ha gestionado su ciberseguridad de diversas formas (reactivas, disuasivas, de ataque o preventivas), generando una multiplicidad de criterios.

Estas dificultades que vemos a nivel global se traducen a nivel regional y vemos como los países sudamericanos no han logrado alcanzar una seguridad cibernética competente para hacerle frente a las nuevas amenazas que se presentan en el ciberespacio. La UNASUR y la OEA, con una cantidad de

miembros muchísimo menor que la de la ONU o la OTAN, no han podido generar criterios comunes, políticas homogéneas y procedimientos efectivos que permitan unir fuerzas y hacerle frente a la ciberguerra y a todos las ciberamenazas como un solo bloque.

El Ecuador al ser parte de redes globales no es ajeno a esta realidad, a pesar de que ha realizado esfuerzos por mejorar sus capacidades dentro de la ciberseguridad, el hecho de no tener un plan de acción unificado para todas las empresas públicas, hace que el país no tenga políticas públicas definidas, de modo que el Ecuador es altamente vulnerable ante ciberataques de toda índole.

En cuanto a detección del responsable de un determinado ataque cibernético en el Ecuador es casi imposible ya que, como lo vimos durante el desarrollo de la investigación, aunque el Comando de Ciberseguridad de las Fuerzas Armadas cuenta con personal certificado en análisis forense digital[43], no cuentan con la capacidad para llevar a cabo un registro de los ciberataque que recibe el país en porque hasta el 2015 no estaban desarrolladas tecnologías, procesos o infraestructura adecuadas.

En el Ecuador se ha hecho inversión en medidas ofensivas cibernéticas más que en medidas defensivas, es decir que se ha priorizado el aspecto de la realización de ataque más que de la defensa o prevención ante las ciberamenazas.

A las Fuerzas Armadas se le ha retirado funciones dentro de la inteligencia y se las ha otorgado a la Secretaría de inteligencia. Esta acción incluye a la ciberdefensa; por lo que, entre las funciones del SENAIN podemos ver que están contempladas acciones de ciberdefensa que contribuyan con la seguridad integral del Estado.

[43]"De manera más formal podemos definir el Análisis Forense Digital como un conjunto de principios y técnicas que comprende el proceso de adquisición, conservación, documentación, análisis y presentación de evidencias digitales y que llegado el caso puedan ser aceptadas legalmente en un proceso judicial. Por evidencia digital se entiende al conjunto de datos en formato binario; comprende los ficheros y las referencias de estos (metadatos) que se encuentren en los soportes físicos o lógicos del sistema atacado." (Delgado M. L., 2007, pág. 5)

El Ecuador también es débil en cuanto a recursos humanos puesto que, pese a que el Ministerio de Defensa en el 2014 anuncio que la malla curricular de todas las instituciones de formación militar avaladas por el SENESCYT iban a tener un cambio con la adición de materias de ciberseguridad y defensa, esto no se ha hecho realidad, de modo que se dificulta formar un equipo capaz de solventar las falencias de ciberseguridad que presenta el país.

Hasta el 2015 podemos ver que el Ecuador cuenta con marcos normativos en materia de ciberseguridad y defensa, pero que no se pueden hacer efectivos ya que no se tiene instituciones calificadas que puedan dar cuenta de los ciberataques que ocurren dentro del países, que no han delimitado cuales son los delitos cibernéticos frecuentes, y que no tienen la suficiente experiencia como para poder realizar un análisis forense que permita determinar a los ejecutores del ciberataque o el lugar desde el que se lo realizo.

En base a lo antes mencionado vemos que la posición que tiene el Ecuador dentro del debate que surge entre la seguridad nacional y los derechos del ciudadanos, se inclina más hacia el lado de los derechos de privacidad del ciudadano, no porque el Estado respete los derechos ciudadanos a carta cabal, sino porque aún no cuenta con las herramientas necesarias para hípervigilar al individuo. Cuando el país cuente con las capacidades necesarias para vigilar completamente a sus ciudadanos, veremos que la balanza cambiará de lado ya que, como vimos en este debate, dentro del marco teórico, los derechos de privacidad del ciudadano interfieren con la seguridad nacional.

A lo largo de esta tesis hemos observado que desde el año 2008 hasta el 2015 el Ecuador ha concebido a la ciberseguridad como parte importante de la seguridad nacional pero no vital, de modo que las iniciativas que se han llevado a cabo para mejorar sus capacidades dentro del ciberespacio no son concretas, integrales ni efectivas. La situación del país no es del todo desoladora ya que hay proyectos

que se encuentran en marcha que van a aportar a la seguridad cibernética, pero debemos estar consciente de que nos falta recorrer un largo camino para poder disuadir, prevenir y hacerle frente a las ciberamenazas.

GLOSARIO

4.1. Ciberamenazas y sus actores

4.1.1. Ciberamenazas

Las ciberamenazas son amenazas planteadas por medio de Internet o el ciberespacio. Según Catwell y Norwood, en su libro "CYBERSECURITY, CYBERANALYSIS AND WARNING" (CATWELL, 2009), las amenazas que se presentan en el ciberespacio son:

Operadores de redes de bots

Las redes de bots son grupos de ordenadores infectados controlados de forma remota por un hacker. En este tipo de ciberamenazas los operadores de red de bots toman varios sistemas para coordinar ataques de phishing, spam y malware. Muchas veces los servicios de estas redes se ponen a disposición de mercados subterráneos.

Grupos criminales

Los grupos criminales atacan a los sistemas para obtener ganancias monetarias. Específicamente, los grupos de delincuencia organizada utilizan spam, phishing y spyware para cometer robo de identidad y fraude en línea. Esta amenaza surge de grupos de espionaje corporativo internacional y grupos de crimen organizado con la capacidad para realizar espionaje industrial y robo monetario a gran escala. Pueden contratar o entrenar a talentosos hackers.

Servicios de inteligencia extranjera

Los servicios de inteligencia utilizan herramientas cibernéticas para recopilar información y espiar a otros Estados. Muchos de estos servicios están trabajando arduamente para desarrollar programas y mejorar sus capacidades

dentro de la guerra de la información. Dichas capacidades permiten que una sola identidad pueda afectar gravemente a un país mediante la interrupción de suministros y comunicaciones o la irrupción en las infraestructuras económicas.

Hackers

Los Hackers buscan obtener acceso no autorizado a una computadora, incluso ahora pueden descargar scripts de ataque y protocolos de internet para lanzarlos contra su víctima. Así las herramientas de ataque se han vuelto cada vez más sofisticadas, también se han vuelto más fáciles de usar. Según la Agencia Central de Inteligencia de los Estados Unidos la mayoría de los hackers no tienen la experiencia necesaria para amenazar redes criticas del Estado, sin embargo la población mundial de hackers si representa una amenaza relativamente alta ya que cuenta con la capacidad para llevar a cabo una irrupción aislada o breve en las máquinas de un Estado y causar graves daños.

Insiders

Los insiders son miembros de las organizaciones que se encuentran descontentos, no necesitan mucho conocimiento acerca de cómo hackear una máquina ya que al ser un miembro de la empresa tiene acceso libre a las maquinas como para causar daños al sistema o robarse información. La complejidad de esta amenaza va más allá del robo de información o el daño del sistema, muchas veces un empleado puede introducir accidentalmente un malware, ya sea mediante el acceso a una página web, a un mail o a un dispositivo electrónico conectado en su máquina.

Phishers

Son individuos o grupos pequeños que ejecutan esquemas de phishing para robar identidades o información y obtener ganancias monetarias. Los phishers también pueden usar spam o spyware para lograr sus objetivos.

Spammers

Son individuos o empresas que mandan correos electrónicos no solicitados con información oculta o falsa para vender productos, realizar esquemas de phishing, distribuir spyware o malware y atacar a las organizaciones o a individuos. Varios virus que se han mandado como spam han dañado archivos y unidades de disco duro de sus víctimas; como ejemplos podemos ver al macro-virus de Melissa, creado por David L. Smith, que infectaba los archivos de Microsoft Word. Este virus llegó a los correos de algunos usuarios como "List.doc" el cual se suponía que contenía 80 claves de sitios web pornográficos. Este virus causó la pérdida de más de 80 millones de dólares por daños a empresas norteamericanas.

Terroristas

Los terroristas buscan destruir, incapacitar o explotar las infraestructuras críticas de un Estado, con el fin de amenazar su seguridad nacional, causar bajas masivas, debilitar la economía de ese país y dañar la moral pública y la confianza. Los grupos terroristas pueden utilizar phishing o spyware para realizar robos y generar fondos o para recolectar información confidencial.

Crimen Organizado

En el ciberespacio existen organización criminales asociadas que utilizan herramientas como phishing, spyware y spam para llevar a cabo transacciones ilícitas (Smith, Lau, & Yiu-Chung, 2015, pág. 69). Muchas de las actividades ilícitas organizadas en internet no se han llevado a cabo por intereses monetarios, también se las efectúa por búsqueda de desafío intelectual, notoriedad individual o grupal, lujuria, ideología, rebelión y curiosidad. Como Ejemplo de este tipo de grupos de crimen organizado tenemos a Wonderlan en el cual sus miembros intercambiaban imágenes ilícitas de niños.

Hacktivismo

Es una práctica de personas o grupos que persiguen el control de redes o sistemas para promover su causa o defender sus posicionamientos políticos o sociales, basados en motivos ideológicos (Centro Criptológico Nacional de España, 2016). Como ejemplo vemos al grupo Anonymous que es un conjunto de anarquistas que se dedica al hacktivismo y cuyos principales objetivos son la Agencia Central de Inteligencia de Estados Unidos, la Iglesia de la Cienciología y la Motion Picture Association of América. Se convirtieron en un apoyo para WikiLeaks (Russell G. Smith, 2015, pág. 70). Esta agrupación se organiza de manera difusa en la red y planifica operaciones, debates acerca de situaciones específicas que ocurren alrededor del mundo y protestas valiéndose de distintos canales en línea.

Ciberespionaje

El ciberespionaje es una modalidad en la que hackers atacan redes computacionales para obtener acceso a información clasificada, rentable y ventajosa (TECHNOPEDIA, 2017). El ciberespionaje es considerado la amenaza cibernética más grande ya que afecta tanto a los individuos como a los Estados y la mayoría de las ciberamenazas antes mencionadas se basan en el espionaje cibernético para atacar.

Individuo

El propio individuo podría en un determinado momento o circunstancia convertirse en una amenaza, cuando con una precaria cultura cibernética y actuando bajo una noción de comunidad de masas se vuelven contra de sus propios elementos, atacando a personas de la red, a través de videos, fotos, palabras, oraciones o símbolos, mensajes falsos, y/o promover el bullying cibernético (Martínez, M, 2014, págs. 138 - 139)

4.1.2. Actores

En este punto es muy amplio el espectro como para poder determinar exactamente los actores que están involucrados en las ciberamenazas, más sin embargo si se ha podido identificar ciertos grupos como actores los cuales según Gian Fiero Siroli citado en (Halpin, Trevorrow, Webb, & Wright, 2006) son:

Hackers genéricos

Estos hackers pueden ser profesionales u aficionados que pasan la mayoría de su tiempo analizando las debilidades y fortalezas de los sistemas informáticos. A menudo los hackers genéricos no tienen motivaciones malévolas simplemente buscan desafiar a su intelecto.

Los iniciados

Este grupo a menudo está involucrado en casos de espionaje industrial, económico o corporativo; por lo general están motivados por el dinero o por venganza, de modo que son una gran amenaza para las organizaciones.

Delincuentes a nivel individual o dentro de organizaciones

Este tipo de delincuentes por lo general son personas que se encuentran insatisfechas dentro de una empresa o que pertenecen a una organización y se infiltran en una empresa para recopilar información confidencial de la competencia.

Grupos estatales y no estatales

Estos grupos suelen tener motivaciones políticas y pueden ser agencias gubernamentales o de inteligencia, unidades militares y hasta grupos terroristas (Dr Edward Halpin, 2006, pág. 42). Los objetivos de estos grupos

pueden ser la recolección de información confidencial, difusión de mensajes mediante propaganda, vigilancia electrónica, censura y sabotaje.

4.2. Definición de estructuras críticas y sus vulnerabilidades

Existen infraestructuras que se han convertido en esenciales para la organización, la funcionalidad y la estabilidad económica de un país desarrollado y moderno, las cuales, según Gian Fiero Siroli citado en (Halpin, Trevorrow, Webb, & Wright, 2006), son:

Sector de información y comunicación

Este sector incluye a todos los equipos de telecomunicación, hardware y software, y las líneas que proporcionan conectividad y servicios de internet.

En el pasado, dentro de este sector, se han documentado varios ataques e intrusiones mediante el bloqueo de softwares de dispositivos de red y de sistemas de gestión. En los últimos años la Red Telefónica Pública Conmutada (RTPC) se ha adentrado en el mundo del software, y está siendo manejada y gestionada remotamente a través de redes informáticas; esto ha aumentado las posibilidades de intrusión electrónica. La vulnerabilidad en este sector ha crecido desde los años 90, ya que dentro de su evolución y despliegue la seguridad de alto nivel no fue vista como primordial.

Los sistemas complejos de producción, almacenamiento y distribución

Estos sistemas complejos manejan recursos como el gas natural, petróleo crudo y refinado, energía nuclear y la energía eléctrica. Estos sistemas son vitales para la estabilidad de la economía de un país por lo que constituyen un claro objetivo frente a la ciberamenazas.

La vulnerabilidad de este sector se ha incrementado por la reciente y rápida proliferación de sistemas informáticos industriales, usando una arquitectura abierta que muchas veces no está provista de software de seguridad para neutralizar una ciberataque. A modo de ejemplo, el uso generalizado de los sistemas de supervisión y adquisición de datos (SCADA), para monitorear y controlar la infraestructura energética, aumenta el riesgo de severos daños y de disturbios causados por ataques cibernéticos.

El sector bancario y financiero

Este sector incluye entidades como bancos, organizaciones comerciales, instituciones de inversión, casas comerciales y organizaciones operativas asociadas. También contempla actividades de apoyo como servicios de transacciones financieras, pagos electrónicos y sistemas de mensajería relacionados.

Las vulnerabilidades del sector bancario y financiero son físicas, por lo que se han tomado medidas fuertes para asegurar la infraestructura y su sistema operativo; sin embargo sigue habiendo un nivel de riesgo debido a la irrupción en los servicios de telecomunicaciones y energía eléctrica. Esta área está en constante riesgo debido a las oportunidades de robo y fraude que presenta. La principal amenaza a la seguridad de las instituciones financieras individuales son los nuevos trabajadores que pueden recopilar información confidencial u operar sistemas con fines de lucro personal.

Sector de distribución física

Este sector comprende todas las vías y puertos navegables, que permiten la movilización de bienes y personas dentro y fuera de las fronteras de un país.

Como en otras áreas, la ciber-vulnerabilidades de este sector se genera por el incremento en el uso de los sistemas inteligentes de movilización y de las

infraestructuras de comunicación. La industria de transporte se ve obligada a utilizar sistemas inteligentes de transporte para optimizar y aumentar su eficiencia, lo cual la hace propensa a ciberataques a gran escala.

Sector del servicio vital humano

Este sector abarca a los servicios de emergencia, servicios de gobierno, agencias estatales y locales, y al servicio de abastecimiento de agua de todo el país.

La vulnerabilidad de este sector radica en la creciente alianza que ha tenido con los sistemas SCADA, es decir que los sistemas SCADA ahora son usados para el control del suministro de agua y algunos servicios de emergencia. Los servicios de gobierno mantienen mega bases de datos que contienen información altamente confidencial sobre sus ciudadanos, y el ciberespionaje al que están expuestas estas bases de datos se debe a su dependencia de la tecnología computacional.

4.3. Siglas

BID: Banco Interamericano de Desarrollo
CCD CoE: Centro de Excelencia Cooperativa de Ciberdefensa de la OTAN
CERT: Centro de Respuesta a Incidentes Informáticos
CIAO: Oficina de Aseguramiento de Infraestructura
CICTE: Comité Interamericano contra el Terrorismo
CITEL: Comisión Interamericana de Telecomunicaciones
COTICDE: Comité de Tecnologías de la Información y Comunicación de la Defensa
CSC: Coordinador de Seguridad Cibernética
FDI: Fuerza de Defensa Israelí
FIRST: Forum of Incident Reponse and Security Teams

ICI-IPC: Comité de Política de Inteligencia de Infraestructuras de Información y Comunicación

INAP: Instituto Nacional de Administración Pública

INAP: Instituto Nacional de Administración Pública de Argentina

IW: Information War

LTTE: Liberation Tigers of Tamil Eelam

MISP: Plataforma de Intercambio de Información sobre Malware

MN CD E & T: Proyecto Multinacional de Educación y Capacitación en Ciberdefensa

MN CD2: Capacidades Multinacionales de Defensa Cibernética

NCISS: Escuela de Sistemas de Información y Comunicaciones de la OTAN

NIAC: National Infraestructura Assurance Council

NIPC: Centro Nacional de Protección de Infraestructuras

NPIIP: Plan Nacional para la Protección de Infraestructura de la Información

NSA: National Security Agency

OEA: Organización de Estados Americanos

ONU: Organización de Naciones Unidas

OTAN: Organización del Tratado del Atlántico Norte

PCCIP: Comisión Presidencial sobre Protección de Infraestructura Crítica

PDD63: Directiva de Decisiones Presidenciales 63

PLA: People´s Liberation Army

SCADA: Supervisory Control And Data Acquisition

SNAP: Secretaría Nacional de la Administración Pública

SUPERTEL: Superintendencia de Telecomunicaciones

TIC: Tecnologías de la Información y la Comunicación

UIT: Unión Internacional de Telecomunicaciones

UNASUR: Unión de Naciones Suramericanas

BIBLIOGRAFÍA

Acosta, O. P., Rodríguez, J. A., Torre, D. A., Ballesteros, & Taboso, P. (2009). *Seguridad Nacional y Ciberdefensa.* Madrid: Fundación Rogelio Segovia para el Desarrollo de las Telecomunicaciones Ciudad Universitaria.

AETecno. (16 de 03 de 2016). *AETecno*. Obtenido de AETecno: http://tecno.americaeconomia.com/articulos/america-latina-el-nuevo-paraiso-de-los-ciberataques

Asamblea Constituyente. (2008). *Asamblea Nacional.* Obtenido de Asamblea Nacional: http://www.asambleanacional.gov.ec/documentos/constitucion_de_bolsillo.pdf

Asamblea Nacional. (10 de 02 de 2014). *CEPAL.* Obtenido de CEPAL: http://oig.cepal.org/sites/default/files/2014_ecu_codpenal.pdf

Banco Interamericano de Desarrollo. (14 de Marzo de 2016). *Banco Interamericano de Desarrollo.* Obtenido de Banco Interamericano de Desarrollo: http://www.iadb.org/es/noticias/comunicados-de-prensa/2016-03-14/informe-sobre-ciberseguridad-en-america-latina,11420.html

Barrueto, L. E. (3 de 12 de 2009). *Maestros del Web*. Obtenido de Maestros del Web: http://www.maestrosdelweb.com/fuera-bombas-titan-rain-seguridad-norteamericana/

Bayuk, J. L., Healey, J., Rohmeyer, P., Sachs, M. H., Schmidt, J., & Weiss, J. (2012). *Cyber Security Policy Guidebook.* New Jersey: A John Wiley & Sons.

Becoña, E. (2006). *Asociacion Española de Psicología Clinica y Psicopatología.* Obtenido de Asociacion Española de Psicología Clinica y Psicopatología: http://aepcp.net/arc/01.2006(3).Becona.pdf

Borbúa, R. V., Herrera, L. R., & Reyes, R. P. (2017). Ciberdefensa y ciberseguridad, más allá del mundo virtual: modelo ecuatoriano de gobernanza en ciberdefensa. *URVIO Revista Latinoamericana de Estudios de Seguridad*, 31-45.

Bravo, D. (26 de 07 de 2015). *EL COMERCIO.* Obtenido de EL COMERCIO: http://www.elcomercio.com/actualidad/ecuador-muestra-vulnerable-ciberataques.html

Bustamante, G. A., Rivera, J. R., & Salinas, S. (21 de 08 de 2017). *Research Gate.* Obtenido de Research Gate:

https://www.researchgate.net/publication/296484484_La_ciberdefensa_como_parte_de_la_agenda_de_integracion_sudamericana_1

Buzan, B. (2008). People, States & Fear: An Agenda for International Security Studies in the post-Cold War Era. *Revista Académica de Relaciones Internacionales, Núm. 9*.

Buzan, B., & Hansen, L. (2009). *The Evolution of International Security Studies.* New York: CAMBRIDGE UNIVERSITY PRESS.

Buzan, B., Waever, O., & de Wilde, J. (1998). *Security, A New Framework for Analysis.* Colorado: Lynne Rienner Publishers.

Cambridge Dictionary. (22 de 05 de 2017). *Cambridge Dictionary*. Obtenido de Cambridge Dictionary: http://dictionary.cambridge.org/es/diccionario/ingles/hegemon

CARI. (2013). *CARI.* Obtenido de CARI: http://www.cari.org.ar/pdf/ciberdefensa_riesgos_amenazas.pdf

Carrasco, L. d. (12 de 2010). *INSTITUTO ESPAÑOL DE ESTUDIOS ESTRATEGICOS.* Obtenido de INSTITUTO ESPAÑOL DE ESTUDIOS ESTRATEGICOS: http://www.ieee.es/Galerias/fichero/docs_opinion/2010/DIEEEO25_2010Wikileaks.pdf

CATWELL, K. T. (2009). *CYBERSECURITY, CYBERANALYSIS AND WARNING.* New York: Nova Science Publishers, Inc.

Centro Criptológico Nacional de España. (18 de 05 de 2016). *CCN-Cert.* Obtenido de CCN-Cert: https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/1483-ccn-cert-ia-0916-ciberamenazas-2015-tendencias-2016-resumen-ejecutivo/file.html

CERT. (12 de 12 de 2016). *CERT*. Obtenido de CERT: http://www.cert.org/about/

Comando Conjunto de las Fuerzas Armadas y Comando de Ciberdefensa. (s.f.). COMANDO DE CIBERDEFENSA. QUITO, PICHINCHA, ECUADOR. MATERIAL NO PUBLICADO.

Computer Science and Telecommunications Board, Division on Engineering and Physical Sciences and National Research Council of EEUU. (2002). *Cybersecurity TODAY and TOMORROW.* Washington: NATIONAL ACADEMY PRESS.

Congreso Nacional. (19 de 11 de 2016). *WIPO.* Obtenido de WIPO: http://www.wipo.int/wipolex/es/text.jsp?file_id=243546

Corrales, L. (12 de 2007). *Escuela Politecnica Nacional.* Obtenido de Escuela Politecnica Nacional: http://bibdigital.epn.edu.ec/bitstream/15000/10020/2/PARTE%202.pdf

Cpnt. Toapanta, E. (2015). LA CIBERSEGURIDAD COMO ESTRATEGIA DE PROTECCIÓN A LA CIUDADANÍA. QUITO, PICHINCHA, ECUADOR.

Delgado, A. (11 de 2014). *Andrés Delgado.* Obtenido de Andrés Delgado: http://delgado.ec/research/es/Gobernanza_Internet_Ecuador_2014.pdf

Delgado, M. L. (06 de 2007). *Organization of American States.* Obtenido de Organization of American States: https://www.oas.org/juridico/spanish/cyb_analisis_foren.pdf

Delgado, R. C., Garcés, M. F., & Dávila, C. L. (2014). *AGENDA POLÍTICA.* Quito.

Departamento de Cooperación Jurídica de la OEA. (02 de 08 de 2017). *Departamento de Cooperación Jurídica de la OEA*. Obtenido de Departamento de Cooperación Jurídica de la OEA: http://www.oas.org/juridico/spanish/cybersp.htm

Días, J. R. (19 de 08 de 2016). *ieee.* Obtenido de ieee: http://www.ieee.es/Galerias/fichero/docs_opinion/2016/DIEEEO86-2016_Ciberamenazas_JRuizDiaz.pdf

Duart, J. M. (02 de 12 de 2008). *UOC.* Obtenido de UOC: http://www.uoc.edu/dt/20173/

EcuCERT. (15 de 05 de 2017). *EcuCERT.* Obtenido de EcuCERT: https://www.ecucert.gob.ec/nosotros.html

EL COMERCIO. (24 de 01 de 2015). *EL COMERCIO.* Obtenido de EL COMERCIO: http://www.elcomercio.com/actualidad/cibermafias-ciberataque-17empresas-ecuador-seguridadinformatica.html

EL COMERCIO. (07 de 03 de 2017). Hoy se analizó el delito informático en Quito. *EL COMERCIO*, págs. http://www.elcomercio.com/actualidad/negocios/hoy-se-analizo-delito-informatico.html.

EL UNIVERSO. (08 de 08 de 2011). *EL UNIVERSO.* Obtenido de EL UNIVERSO: http://www.eluniverso.com/2011/08/09/1/1431/ecuador-preparado-posibles-ataques-informaticos.html

EL UNIVERSO. (20 de 06 de 2011). *EL UNIVERSO.* Obtenido de EL UNIVERSO: http://www.eluniverso.com/2011/06/20/1/1355/pagina-internet-presidencia-ecuatoriana-sufrio-ataque-informatico.html

EL UNIVERSO. (29 de 06 de 2012). *EL UNIVERSO.* Obtenido de EL UNIVERSO: http://www.eluniverso.com/2012/06/29/1/1356/bancos-deben-tener-seguros-contra-delitos-informaticos.html

EL UNIVERSO. (09 de 09 de 2014). *EL UNIVERSO.* Obtenido de EL UNIVERSO: http://www.eluniverso.com/noticias/2014/09/09/nota/3805401/ffaa-anuncian-2015-comando-operaciones-ciberdefensa

FIRST. (05 de 05 de 2017). *FIRST*. Obtenido de FIRST: https://www.first.org/about/mission

Foro Económico Mundial. (24 de 04 de 2017). *World Economic Forum.* Obtenido de World Economic Forum: http://www3.weforum.org/docs/WEF_GlobalInformationTechnology_Report_2014.pdf

Freedom House. (02 de 11 de 2016). *ECOI.* Obtenido de ECOI: https://www.ecoi.net/local_link/314187/452551_de.html

García, L. F. (2013). *Cuaderno de la Guardia Civil.* Obtenido de Cuaderno de la Guardia Civil: http://intranet.bibliotecasgc.bage.es/intranet-tmpl/prog/local_repository/documents/15310.pdf

González, J. C. (2016). LOS CERTs COMO HERRAMIENTA DE APOYO A LA CIBERDEFENSA EN LAS FF.AA. *Revista de Ciencias de Seguridad y Defensa*, 17-23.

Halpin, D. E., Trevorrow, D. P., Webb, P. D., & Wright, D. S. (2006). *Cyberwar, Netwar and the Revolution in Military Affairs.* New York: PALGRAVE MACMILLAN.

IMPACT. (22 de 06 de 2017). *IMPACT*. Obtenido de IMPACT: http://www.impact-alliance.org/aboutus/ITU-IMPACT.html

INEC. (2008). *INEC.* Obtenido de INEC: http://www.ecuadorencifras.gob.ec/documentos/web-inec/Estadisticas_Sociales/TIC/2008/Presentacion_de_resultados_2008.pdf

INEC. (2015). *INEC.* Obtenido de INEC: http://www.ecuadorencifras.gob.ec/documentos/web-inec/Estadisticas_Sociales/TIC/2015/Presentacion_TIC_2015.pdf

International Business Times. (08 de 08 de 2017). Anonymous Continue Hacking Rampage: Ecuador Police Hit. *International Business Times*, pág. http://www.ibtimes.com/.

ITU, T. S. (04 de 2008). *NATO Cooperative Cyber Defence Centre of Excellence.* Obtenido de NATO Cooperative Cyber Defence Centre of Excellence: https://ccdcoe.org/sites/default/files/documents/ITU-080418-RecomOverviewOfCS.pdf

ITU, Unión Internacional de Telecomunicaciones. (15 de 05 de 2017). *ITU.* Obtenido de ITU: www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2007-MSW-S.doc

javcasta Wordpress. (28 de 09 de 2016). *javcasta*. Obtenido de javcasta: https://javcasta.files.wordpress.com/2009/09/lenguaje-de-comandos-e28093-scripts-cmd-bat.pdf

Jefe de Estado Mayor del Comando de Ciberseguridad. (23 de 08 de 2017). Comando de Ciberdefensa. (F. S. Flores, Entrevistador)

Jehangir, H. (19 de 02 de 2012). *E-International Relations Student.* Obtenido de E-International Relations Student: http://www.e-ir.info/2012/02/19/realism-liberalism-and-the-possibilities-of-peace/

Justribó, L. C. (26,27 y 28 de 11 de 2014). *Congreso UNLP.* Obtenido de Congreso UNLP: http://www.congresos.unlp.edu.ar/index.php/CRRII/CRRIIVII/paper/view/1849/422

Kaspersky Lab. (25 de 07 de 2017). *Kaspersky*. Obtenido de Kaspersky: https://www.kaspersky.com/about

Kshetri, N. (2013). *Cybercrime and Cybersecurity in the Global South.* New York: Palgrave Mcmillan.

Kuehl, D. T. (2009). From Cyberspace to Cyberpower: Defining the Problem. En S. H. Franklin D. Kramer, *Cyberpower and National Security* (pág. Capitulo 2). Nebraska: Potomac Books, University of Nebraska Press.

La República. (17 de 09 de 2014). *La República.* Obtenido de La República: http://www.larepublica.ec/blog/sociedad/2014/09/17/ecuador-busca-capacitacion-militar-y-transferencia-tecnologica-de-china/

LACNIC. (17 de 07 de 2017). *LACNIC*. Obtenido de LACNIC: http://www.lacnic.org/web/lacnic/acerca-lacnic

Leiva, E. A. (2015). Estrategias Nacionales de Ciberseguridad: Estudio Comparativo Basado en Enfoque Top-Down desde una Visión Global a una Visión Local. *Revista Latinoamericana de Ingeniería de Software*, 161-176. Obtenido de Revista Latinoamericana de Ingeniería de Software.

Lemieux, F. (2015). *Current and Emerging Trends in Cyber Operations.* Londres: PALGRAVE MACMILLAN.

Lewis, L. (27 de 05 de 2011). *The Australian.* Obtenido de The Australian: http://www.theaustralian.com.au/business/technology/chinas-blue-army-could-conduct-cyber-warfare-on-foreign-powers/news-story/5ebbec95bc758f8f214328d71a42ee5b

LIEBELSON, D. (02 de 07 de 2013). *MotherJones.* Obtenido de MotherJones: http://www.motherjones.com/politics/2013/07/hacker-jester-targets-assange-snowden-ecuador/

Medero, G. S. (2010). LOS ESTADOS Y LA CIBERGUERRA. *Boletín de Información (Ministerio de Defensa de España)*, 63-76.

Medero, G. S. (2012). *Dialnet.* Obtenido de Dialnet: file:///C:/Users/Usuario/Downloads/Dialnet-LosEstadosYLaCiberguerra-3745519%20(2).pdf

Medero, G. S. (11 de 2012). La ciberguerra: los casos de Stuxnet y Anonymous. *Derecom*, 124-133. Obtenido de Dialnet: file:///C:/Users/Usuario/Downloads/Dialnet-LaCiberguerra-4331298%20(1).pdf

Medina, P. (2007). LA ASISTENCIA MILITAR ESTADOUNIDENSE Y LA EVOLUCIÓN DE LAS FUERZAS ARMADAS Y LA POLÍTICA DE DEFENSA DEL ECUADOR. (Tesis de Maestría). *Universidad Andina Simón Bolivar.* Obtenido de: http://repositorio.uasb.edu.ec/bitstream/10644/780/1/T505-MRI-Medina-La%20aistencia%20militar%20estadounidense%20y%20la%20evoluci%C3%B3n%20de%20las%20Fuerzas%20Armadas%20y%20la%20pol%C3%ADtica.pdf

Ministerio de Defensa Nacional. (24 de 09 de 2014). Acuerdo Institucional 281. *Acuerdo Institucional*. Quito, Pichincha, Ecuador. MATERIAL NO PUBLICADO

Ministerio de Defensa Nacional. (29 de 09 de 2016). *Ministerio de Defensa Naciona.* Obtenido de Ministerio de Defensa Naciona: http://www.defensa.gob.ec/wp-content/uploads/downloads/2015/06/Plan-Anual-de-Inversion-MIDENA_mayo_2015.pdf

Ministerio de Relaciones Exteriores y Movilidad Humana. (03 de 06 de 2017). *Ministerio de Relaciones Exteriores y Movilidad Humana.* Obtenido de Ministerio de Relaciones Exteriores y Movilidad Humana: http://www.cancilleria.gob.ec/historia-de-chevron-texaco-en-ecuador/

Morán, D. R. (01 de 04 de 2015). *Instituto Español de Estudios Estratégicos.* Obtenido de Instituto Español de Estudios Estratégicos: http://www.ieee.es/Galerias/fichero/docs_informativos/2015/DIEEEI02-2015_VisionInternacional_Ciberseguridad_DRM.pdf

Morrison, I. H. (11 de 24 de 2014). El presidente de Ecuador acusa ciberataque desde el extranjero. *Audiencia Electronica*.

Mueller, P., & Yadegari, B. (2012). *The University of Arizona.* Obtenido de The University of Arizona: https://www2.cs.arizona.edu/~collberg/Teaching/466-566/2012/Resources/presentations/2012/topic9-final/report.pdf

Naciones Unidas. (2016). *Administración Pública y Gestión del Desarrollo Departamento de Asuntos Económicos y Sociales de la ONU.* Obtenido de Administración Pública y Gestión del Desarrollo Departamento de Asuntos Económicos y Sociales de la ONU: http://workspace.unpan.org/sites/Internet/Documents/UNPAN96407.pdf

OBSERVATORIO DE LA CIBERSEGURIDAD EN AMÉRICA LATINA Y EL CARIBE. (2016). *Ciberseguridad ¿Estamos preparados en América Latina y el Caribe? / Informe Ciberseguridad 2016.* Copyright.

OEA ; BID. (11 de 11 de 2016). *Banco Interamericano de Desarrollo.* Obtenido de Banco Interamericano de Desarrollo: https://publications.iadb.org/handle/11319/7449?locale-attribute=es&

Organización de los Estados Americanos. (19 de 06 de 2016). *symantec.* Obtenido de symantec: https://www.symantec.com/content/es/mx/enterprise/other_resources/b-cyber-security-trends-report-lamc.pdf

Ortega, J. (24 de 06 de 2015). *EL COMERCIO.* Obtenido de EL COMERCIO: http://www.elcomercio.com/actualidad/cibermafias-ciberataque-17empresas-ecuador-seguridadinformatica.html

OTAN. (27 de 02 de 2017). *OTAN.* Obtenido de OTAN: http://www.nato.int/cps/en/natohq/topics_78170.htm#

Oxford Living Dictionaries. (12 de 10 de 2016). *Oxford Living Dictionaries*. Obtenido de Oxford Living Dictionaries: https://es.oxforddictionaries.com/definicion/informatizacion

Panda Lab. (02 de 03 de 2017). *Panda Lab.* Obtenido de Panda Lab: http://www.pandasecurity.com/mediacenter/pandalabs/pandalabs-neutralized-75-million-new-malware-samples-2014-twice-many-2013/

Parks, P. J. (2013). *Ciberwarfare.* United States: ReferencePoint Press, Inc.

Pérez, F. P. (2005). *Teoría del Estado.* México: Porrúa.

Pernik, P., Wojtkowiak, J., & Verschoor-Kirss, A. (2016). *NATO Coperative Cyber Defence Center of Excellence.* Obtenido de NATO Coperative Cyber Defence Center of Excellence: https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_USA_122015.pdf

Peralvo, C. E. (2015). "ESTUDIO PROSPERTIVO DE LA CIBERDEFENSA EN LAS FUERZAS ARMADAS DEL ECUADOR" *.(Tesis de pregrado)*. ESPE. Recuperada de: https://repositorio.espe.edu.ec/bitstream/21000/11583/1/T-ESPE-049543.pdf

Presidential Decision Directives (PDD63). (22 de 05 de 2016). *Federation of American Scientists*. Obtenido de Federation of American Scientists: https://fas.org/irp/offdocs/pdd/pdd-63.htm

Ramos, M. (09 de 2014). *ALAINET.* Obtenido de ALAINET: http://www.alainet.org/images/Acerca%20soberania%20Ecuador%20en%20ciberespacio.pdf

Raska, M. (2015). *Confronting Cybersecurity Challenges: Israel´s Evolving Cyber Defence Strategy.* RSiS.

Real Instituto Elcano. (11 de 11 de 2013). *Real Instituto Elcano.* Obtenido de Real Instituto Elcano: http://www.realinstitutoelcano.org/wps/wcm/connect/7366288041c9aefda642ae709b5c3216/ARI41-2013-THIBER-NSA-espionaje-publico-privada-Snowden.pdf?MOD=AJPERES&CACHEID=7366288041c9aefda642ae709b5c3216

Rogers, A. (07 de 11 de 2013). Ecuador minister decries "first world" cyber attack in presidential elections. *BNamericas*.

Romero, A., Ronquillo, J., Tituana, G., & Aranda, I. A. (21 de 07 de 2011). *ESPOL.* Obtenido de ESPOL:

http://www.dspace.espol.edu.ec/bitstream/123456789/16582/1/Dise%C3%B1o%20y%20Operaci%C3%B3n%20del%20Primer%20CERT.pdf

Secretaría de Inteligencia. (09 de 07 de 2017). *Secretaría de Inteligencia.* Obtenido de Secretaría de Inteligencia: http://www.inteligencia.gob.ec/estrategias/

Secretaría Nacional de la Administración Públlica. (27 de 07 de 2017). *Secretaría Nacional de Administración Públlica.* Obtenido de Secretaría Nacional de Administración Públlica: http://www.administracionpublica.gob.ec/wp-content/uploads/2017/04/Plan-Gobierno-Electronico-V1.pdf

Secretaría Nacional de la Administración Pública. (25 de 09 de 2013). *Administración Pública.* Obtenido de Administración Pública: http://www.administracionpublica.gob.ec/wp-content/uploads/downloads/2016/02/Esquema-Gubernamental-de-Seguridades-de-la-Informacion.pdf

SeguInfo. (23 de 11 de 2016). *Segu.Info.* Obtenido de Segu.Info: http://www.segu-info.com.ar/malware/phishing.htm

Shakarian, M. P. (01 de 2012). *Research Gate.* Obtenido de Research Gate: https://www.researchgate.net/publication/230898141_Stuxnet_Revolucion_de_Ciberguerra_en_los_Asuntos_Militares

Smith, R. G., Lau, R. C.-C., & Yiu-Chung, L. (2015). *Cybercrime Risks and Responses.* Londres: PALGRAVE MACMILLAN.

Stiennon, R. (2010). *SURVIVING CYBERWAR.* Toronto: THE SCARECROW PRESS, INC.

SUPERTEL. (13 de 08 de 2016). *arcotel.* Obtenido de arcotel: http://www.arcotel.gob.ec/wp-content/uploads/2015/02/informe_rendicion_cuentas_2014-1.pdf

TECHNOPEDIA. (26 de 04 de 2017). *TECHNOPEDIA*. Obtenido de TECHNOPEDIA: https://www.techopedia.com/definition/27101/cyberspying

TechTarget. (Junio de 2007). *TechTarget*. Obtenido de TechTarget: http://searchsecurity.techtarget.com/definition/mail-bomb

telesur. (12 de 04 de 2016). *telesur.* Obtenido de telesur: https://www.telesurtv.net/telesuragenda/Estrategia-de-Panama-Papers-20160412-0028.html

The Editors of Encyclopædia Britannica. (10 de 09 de 2015). *Encyclopædia Britannica*. Obtenido de Encyclopædia Britannica: https://www.britannica.com/topic/Tamil-Tigers

The Editors of Encyclopædia Britannica. (02 de 03 de 2017). *Encyclopædia Britannica*. Obtenido de Encyclopædia Britannica: https://www.britannica.com/topic/Peoples-Liberation-Army-Chinese-army

The Free Dictionary. (28 de 07 de 2017). *The Free Dictionary*. Obtenido de The Free Dictionary: http://es.thefreedictionary.com/encriptar

The White House. (25 de 08 de 2017). *The White House.* Obtenido de The White House: https://www.whitehouse.gov/issues/foreign-policy/cybersecurity

ÚLTIMA HORA. (31 de 04 de 2016). LAS AMENAZAS DE CIBERATAQUES PARA ECUADOR OCUPA EL OCTAVO LUGAR ENTRE LOS PAÍSES DE LA REGIÓN. *ÚLTIMA HORA*, págs. http://ultimahoraec.com/las-amenazas-de-ciberataques-para-el-pais-ocupa-el-octavo-lugar-entre-los-paises-de-la-region/.

Urueña, F. J. (09 de 2015). *Instituto Español de Estudios Estratégicos.* Obtenido de Instituto Español de Estudios Estratégicos: http://www.ieee.es/Galerias/fichero/docs_opinion/2015/DIEEEO09-2015_AmenazaCiberataques_Fco.Uruena.pdf

Ventre, D. (2014). *Chinese Cybersecurity and Defense.* Hoboken: Wiley.

Weber, R. H., & Heinrich, U. I. (2012). *Anonymization.* London, Heidelberg, New York and Dordrecht: Springer.