CIBERSEGURIDAD Y CIBERDEFENSA: ¿QUÉ IMPLICACIONES TIENEN PARA LA SEGURIDAD NACIONAL?

EDISSON MAURICIO VARGAS VARGAS

UNIVERSIDAD MILITAR NUEVA GRANADA
FACULTAD DE RELACIONES INTERNACIONALES, ESTRATEGIA Y SEGURIDAD
ESPECIALIZACIÓN EN ALTA GERENCIA DE LA DEFENSA NACIONAL
BOGOTÁ D.C.
2014

CIBERSEGURIDAD Y CIBERDEFENSA: ¿QUÉ IMPLICACIONES TIENEN PARA LA SEGURIDAD NACIONAL?

EDISSON MAURICIO VARGAS VARGAS

Trabajo de grado para optar al título de Especialista en Alta Gerencia de la Defensa Nacional

UNIVERSIDAD MILITAR NUEVA GRANADA
FACULTAD DE RELACIONES INTERNACIONALES, ESTRATEGIA Y SEGURIDAD
ESPECIALIZACIÓN EN ALTA GERENCIA DE LA DEFENSA NACIONAL
BOGOTÁ D.C.
2014

RESUMEN

CIBERSEGURIDAD Y CIBERDEFENSA: ¿QUÉ SON Y QUÉ IMPLICACIONES TIENES PARA LA SEGURIDAD DE UN PAÍS?

Se vive en una era en donde la información va de la mano junto con la tecnología. De allí que ahora la población en general puede acceder a una cantidad significativa de información en tan solo unos pocos segundos, sin importar la distancia que separe a un país de otro. Así mismo, no solo el flujo de información manda la parada en una sociedad cada vez más globalizada, es importante tener en cuenta la tecnificación de bienes y servicios que ahora funcionan por medio de computadoras a través del ciberespacio.

Este trabajo estudiará los conceptos de ciberseguridad y ciberdefensa, las distintas amenazas latentes en el ciberespacio, los programas y políticas que los países diseñan para evitar ataques cibernéticos, y en la actualidad qué está desarrollando Colombia para ser lo menos vulnerable posible en materia de seguridad en la red.

Palabras Clave

Ciberseguridad, ciberdefensa, ciberguerra, mecanismos de defensa, ciberespacio.

ABSTRACT

CIBERSECURITY AND CIBERDEFENSE: WHAT ARE THEY AND WHAT IMPLICATIONS DO THEY HAVE FOR HOME SECURITY?

We live in an era where information and technology are together. Now people can access to the biggest amount of information in just a few seconds, no matter the distance between countries on the world. Moreover, information flow is not the only thing that is important in a society increasingly globalized; It is important consider goods and services modernization that work with computers through the cyberspace.

This paper will study cybersecurity and cyberdefense concepts, the different ways of threats on cyberspace, programs and policies that countries design for avoiding cybernetic attacks, and in the present what Colombia is developing to be as less vulnerable as possible in the topic of network security.

Key words

Cybersecurity, cyberdefense, cyberwar, prevention, defense mechanisms, cyberspace

INTRODUCCIÓN

Los campos en los que se enfrenta una guerra pueden ser por aire, mar, tierra y hasta en el mismo espacio, como lo nombra el Instituto Español de Estudios Geoestratégicos (2011). Sin embargo, debido a los acontecimientos de los últimos años, en cuanto a seguridad informática y ataques cibernéticos, incluyendo la filtración de cables diplomáticos estadounidenses en internet a través del portal wikileaks, y la información brindada por el ex funcionario de la CIA, Edward Snowden (BBC Mundo, 2013), provoca una reflexión acerca de si el mundo se encuentra frente a un nuevo campo de batalla; que implicaciones tiene y las posibles repercusiones que puede tener para un país en materia de seguridad y defensa, en especial en el caso colombiano.

"Las tecnologías informáticas transforman nuestra manera de pensar y actuar en cualquier aspecto de nuestras vidas, introduciendo importantes cambios estructurales, al permitirnos modelar objetos de todo tipo en forma de información, permitiendo de este modo su manipulación por medios electrónicos" (Unión Internacional de Telecomunicaciones, ITU. 2007. P.3). Es por esta razón que el mundo es cada vez más dependiente de la tecnología, más puntualmente a la internet, lo cual, hace a los Estados más vulnerables a un ciberataque, que puede poner en jaque estructuras criticas de un Estado, ya sea en su parte militar y no menos importante, infraestructura que puede afectar directamente a la población civil sin necesidad de disparar una sola bala.

El objetivo principal de este trabajo es demostrar cómo la ciberseguridad y la ciberdefensa permite evidenciar que en el ciberespacio existen amenazas latentes a la seguridad de un estado o una organización. A lo largo del mismo, se busca ofrecer una explicación sobre estos términos, y que sea lo más sencillo posible. Se ha realizado una compilación de varios documentos que hablan sobre el tema. Para ello, se dividirá este trabajo en tres grandes capítulos. El primero trata sobre la terminología básica sobre ciberseguridad, ciberdefensa, ciberguerreros, y los distintos métodos en que se utiliza la red, ya sea para atacar a un enemigo o proteger información valiosa. Será una especie de estado del arte sobre el tema de ciberseguridad

y ciberdefensa. Y explicando de la manera más simple el funcionamiento de sistemas que son útiles para acceder a redes privadas y realizar ataques informáticos.

El segundo capítulo, hablará sobre los distintos ataques cibernéticos que se han desatado en los países más importantes del mundo, teniendo en cuenta modus operandi, y las consecuencias que trajeron estos ciberataques. También tratará sobre los distintos métodos que algunos de los países más importantes adoptan para proteger su ciberespacio.

Por último, el tercer capítulo tratará sobre cómo se está preparando Colombia para prevenir este tipo de ataques y que políticas se están implementando, partiendo de lo revisado en el segundo capítulo sobre países que se encuentran a la vanguardia en este tipo de investigaciones sobre la materia, más aún, teniendo en cuenta que aún se vive un conflicto interno, y este tipo de "arma" puede llegar a manos tanto de los grupos al margen de la ley, así como de otros países que pueden atacar desde el ciberespacio sin la necesidad de una confrontación bélica.

CAPITULO 1

BREVE ESTADO DEL ARTE SOBRE CIBERSEGURIDAD Y CIBERDEFENSA

El Ciberespacio

El ciberespacio se puede interpretar como las acciones que una persona común y corriente puede hacer a través de internet, como conectarse con sus amigos por redes sociales, enviar emails, o realizar video llamadas. Es verdad que Internet es parte del ciberespacio pero no lo es todo.

Clarke y Knake (2011), proponen:

> El ciberespacio lo conforman todas las redes informáticas del mundo y todo lo que ellas conectan y controlan. No se trata solo de internet. Es importante dejar en claro la diferencia. Internet es una red de redes abierta. Desde cualquier red de internet, podemos comunicarnos con cualquier ordenador conectado con cualquiera otra de las redes de internet. El ciberespacio es Internet más montones de otras redes de ordenadores a las que, se supone, no es posible acceder desde internet. Algunas de esas redes privadas son muy semejantes a internet, pero, al menos teóricamente, se encuentran separadas de ella. (pág. 104)

Con esto se vislumbra que a través del ciberespacio se realizan la mayoría de actividades normales de un ser humano, y que un ataque cibernético podría cambiar sustancialmente el estilo de vida de los pobladores de un país en caso de ser atacados los proveedores de servicios públicos, los clientes de un banco, y en casos de mayor envergadura, poner en jaque la seguridad de un Estado. Internet sería entonces el canal de comunicación en el ciberespacio. Surge entonces la pregunta ¿Qué tan dependientes son las personas del ciberespacio hoy en día? La dependencia al ciberespacio ha sido orquestada a partir de la tecnificación de los Sistemas de Información y Comunicaciones (TIC) (Caro. 2011), una vez la información se digitaliza, los niveles de vulnerabilidad en la red se hacen mayores, quedando a merced de quien tenga la

capacidad de ingresar en los sistemas internos y adquirir la información que desee. Como se sabe quien posee la información posee el poder. El ciudadano de a pie, puede brindar su información en el momento en que realiza una transferencia bancaria a través de internet, o solicitar documentos importantes a través de la red, obviamente las empresas y toda entidad que maneje información digitalizada debería tener ciertos protocolos para la seguridad de la información de sus clientes y usuarios en general. Pero, ¿Cómo es posible acceder a información importante o sabotear infraestructura critica de un Estado?

Adrianna Llongueras Vicente (2013) realiza un análisis sobre lo que el ciberespacio representa para la seguridad nacional de un Estado:

> El ciberespacio es un elemento de poder dentro la seguridad nacional, es a través de este nuevo y artificial dominio que se ejerce una innovadora influencia estratégica en el siglo XXI; en este mundo virtual hasta los actores más modestos pueden ser una amenaza para las grandes potencias forjándose y desarrollándose el concepto de las operaciones militares centradas en redes (Pág. 19)

Se hace evidente que a través del ciberespacio cualquier Estado que en términos de una guerra convencional pueda ser el poder blando, o Estado más débil, puede encontrar una ventaja a través del manejo que pueda dar a las ventajas que proporciona el óptimo manejo del ciberespacio y dar en puntos vulnerables al poder duro o Estado más fuerte.

Llongueras (2013) realiza una clasificación básica sobre los ataques que se pueden perpetrar en la red como ataques de alta y baja intensidad.

El ataque de alta intensidad se califica según esta autora como aquel que tiene como objetivo equipamientos militares o infraestructuras críticas que traería como respuesta una acción bélica departe de es agredido. Según Llongueras es mucho más fácil identificar al agresor en este tipo de ataque. El ataque de baja intensidad es el más común que se presenta, dado que representa los delitos como robo de identidad o suplantación, ataques a páginas web y ataques a la información bancaria y robo de dinero por vía electrónica.

Ciberguerreros, ¿Cómo actúan y de qué herramientas disponen para acceder a sistemas vitales de una nación o institución?

Los ciberguerreros son aquellos individuos que con su conocimiento pueden diseñar programas y ciberarmas capaces de infiltrar el sistema de ya sea una organización o entidad, y con esto acceder a información confidencial, colocar bombas lógicas y sabotear el correcto funcionamiento de los flujos de información ya sea de una página de internet, hasta el funcionamiento de la red eléctrica de una ciudad o hasta un país entero. Muchos pueden definir a los ciberguerreros como los individuos que realizan estas acciones y están adscritos a la fuerza militar de un Estado determinado, sin embargo no son los únicos en capacidad de conocer software y hardware y ocasionar daños importantes, también existen comunidades de "geeks", que son personas interesadas en el estudio de software y hardware, las cuales se especializan en detectar fallos de sistemas operativos y demás software; unos con propósitos académicos, otros con el fin de perjudicar empresas y gobiernos. María José Caro (2011, p. 72), hace una clasificación de los tipos de atacantes que se encuentran en el ciberespacio.

- Atacantes patrocinados por Estados
- Servicios de Inteligencia y Contrainteligencia
- Terrorismo, extremismo político e ideológico
- Ataques de delincuencia organizada
- Ataques de perfil bajo

Por esta razón, los países industrializados y que están a la vanguardia en tecnología, como Estados Unidos, Rusia, China entre otros, buscan ostentar el dominio del ciberespacio tanto para el ataque como para la defensa teniendo en cuenta que el factor tiempo en el ciberespacio da un intervalo desde un par de minutos hasta milésimas de segundo para realizar un ataque (Caro, M. 2011). Para ello, un ciberguerrero puede emplear distintos métodos para acceder a los sistemas y conseguir su cometido. Por eso, Luis Joyanes (2011) enumera los siguientes:

Stuxnet

Es un programa malicioso que permite introducirse en los sistemas que controlan infraestructuras críticas como oleoductos entre otras con el fin de sabotear el funcionamiento de dichas infraestructuras haciendo que estas se apaguen u otras acciones dependiendo la estructura que se quiera atacar.

DDoS

Los ataques DDoS (Distributed Denial of Service) son los ataques más comunes que puede tener una página web, que consiste en saturar los servidores web de una institución hasta el punto que esta misma colapse, para esto se utilizan computadoras que se encuentren infectadas por virus (botnets) haciendo que se cree una red, en esta red de computadoras infectadas, los usuarios no se dan cuenta que hacen parte del ataque.

Botnets

Los botnets (robots de la Red) son redes de computadoras utilizadas para dirigir un ataque DDoS. Esto se da por ejemplo, cuando una persona del común abre u correo basura o Spam, este correo se encuentra infectado de virus haciendo que la maquina este a merced de los hackers o ciberguerreros. Joyanes (2011) indica que este tipo de ataque es utilizado con el fin de espiar corporaciones e instituciones gubernamentales.

Zeus

Zeuz es un virus comúnmente conocido como troyano que se encarga de ingresar a las computadoras de los usuarios con el fin de obtener contraseñas de redes sociales, información bancara entre otra con el fin de realizar acciones de suplantación y robos a cuentas bancarias tarjetas de crédito etc

Según Clarke y knake (2011, P. 108 - 123), “existen al menos seis vulnerabilidades importantes en el diseño mismo de internet”:

Esas vulnerabilidades son:

- El sistema de direcciones que se utiliza para determinar cómo llegar a una ubicación determinada en la red.
- El enrutamiento entre ISP (Internet Service Provider), un sistema conocido como Protocolo de Puerta de Enlace de Frontera o (BGP Border Gateway Protocol).
- La ICCAN.
- En internet casi todo lo que se hace es abierto, sin codificar.
- Capacidad para propagar de forma intencional para propagar trafico malicioso diseñado para atacar los ordenadores.
- Es una gran red con diseño descentralizado.

El sistema de direcciones que se utiliza para determinar cómo llegar a una ubicación determinada en la red.

Ellos califican las ISP son como “carriers”, dado que son las compañías que transportan el tráfico de internet. Otras son las compañías que fabrican los elementos para tener acceso como los routers, el software entre otros, pero los ISP son quienes conectan todo ello.

Clasifican a los ISP en don grandes ramas; Los ISP nacionales que son los grandes proveedores del servicio y administran cientos de kilómetros de cables de fibra óptica, y los ISP más pequeños que gestionan servicio para localidades pequeñas y que se valen de las redes de los grandes proveedores de servicio. Para ello estos expertos proporcionan el siguiente ejemplo de cómo funciona:

> (…)Para empezar, abro un "navegador" en mi portátil. Sólo con abrir el navegador, ya estoy solicitando a mi ordenador que se conecte a internet y cargue mi "página de inicio". Supongamos que esa "página de inicio" es la de la empresa de consultoría para la que trabajo. (Pág. 109)

El autor explica que como los ordenadores no pueden entender las direcciones en internet como "micompañia", hay una serie de traducciones a los lenguajes binarios de programación de los ordenadores denominados como Sistema de nombres de Dominio.

> Mi empresa de consultoría tiene su sede principal a ciento veinte kilómetros de mi casa en Virginia, pero su página web se aloja en un servidor remoto en Minneapolis, cuya dirección de internet es, por decir algo, 123.45.678.90. Esos son muchos números para memorizar. Por suerte, no tengo que hacerlo. El navegador usa el Sistema de Nombres de Dominio para buscar la dirección. El navegador envía un mensaje a una base de datos guardada en un servidor, un componente de la elaborada jerarquía de ordenadores que conforman juntos el Sistema de nombres de Dominios. (Pág. 110)

Para los ciberguerreros el Sistema de nombres de dominios es un blanco, dado que según los autores, este sistema fue creado de manera poco segura y en consecuencia permite a los hackers cambiar cierta información y dirigir al usuario a páginas falsas (Clarke, Knake. 2011).

Vale la pena mencionar que este tipo de movimientos en la red, sobre recorrer más de tres mil kilómetros para poder ingresar a una página de internet a través de los cables de fibra óptica y de red que tienen los ISP, se realizó en tan solo segundos. Pero, ¿Qué oportunidades puede tener alguien que quiera cometer alguna acción contra esta página? Para explicar esto, Richard Clarke, quien fuera el responsable de seguridad con cuatro presidentes de Estados Unidos (Clarke, Knake. 2011), aporta lo siguiente:

> Si un ciberguerrero hubiera querido enviar esos paquetes al lugar equivocado, o impedirle a cualquier parte, tuvo al menos dos oportunidades. Primero, […] pudo haber atacado el Sistema de nombres de Dominio, el servicio de información telefónica de internet, y enviarme a una página equivocada, quizás una falsificación convincente de la web de mi compañía, en la que yo hubiera entrado mi número de usuario y la clave de mi cuenta. Sin embargo, en lugar de penetrar

> ilegalmente en el Sistema de nombres de Dominio para secuestrar mi solicitud, el ciberguerrero pudo haber atacado el sistema mismo. (Pág. 112)

Poniendo en contexto esta primera vulnerabilidad, se aprecia que se asemeja a lo que sucede cuando una persona no ingresa la dirección exacta de un banco, por consiguiente se puede ingresar a una página falsa y es allí donde usurpan nuestra información bancara tal como número de cuenta, claves de acceso para transacciones electrónicas, y de ese modo robar el dinero que se encuentre depositado en la cuenta. Oscar Pastor Acosta, José Antonio Pérez Rodríguez, Daniel Arnáiz de la Torre y Pedro Taboso Ballesteros (2009), aseguran que internet se ha perfilado como una de las nuevas formas de financiación de grupos de mafias y terrorismo que utilizan fraudes con tarjetas de crédito y robo a cuentas bancarias como medio para captar dinero y sostener el accionar de dichos grupos.

El enrutamiento entre ISP (Internet Service Provider), un sistema conocido como Protocolo de Puerta de Enlace de Frontera o (BGP Border Gateway Protocol).

"El BGP es el principal sistema empleado para dirigir los paquetes hacia su destino a lo largo y ancho de internet" (Clarke et al. 2011, p.113). Según esto, el BGP es el intermediario entre el ISP y la página web. Entre sus funciones Clarke menciona que este sistema funciona para enrutar redes distintas mediante un sistema de instrucciones que tiene. Esto debido a que cada red tiene un equipo o router que permite la conexión, y en este sentido lo que hace el sistema es armonizar esas conexiones. Sin embargo no hay un mecanismo que proteja al BGP en contra de ataques que busquen descontrolas el tráfico en internet.

Se infiere entonces, que el GPB si bien es un mecanismo que controla o permite realizar un filtro entre los paquetes que van de un lado a otro en la red, no es suficiente para poder hacer de internet algo seguro. Que cualquier persona con los conocimientos necesarios para ingresar ilegalmente al sistema, puede detener internet, y por razón de la dependencia que el

mundo tiene por el ciberespacio, causaría la pérdida de miles de millones de dólares y obviamente desataría un caos gigantesco.

La ICCAN.

Las decisiones sobre el Sistema de Nombres de Dominio la toma una organización internacional no gubernamental llamada Corporación de Internet para la Asignación de Nombres y Números (ICANN por sus siglas en Inglés) (Clarke et al. 2011). Joyanes (2011) hace una breve descripción de las funciones de la ICANN a saber:

> ICANN no controla el contenido de Internet, no puede detener el correo basura y no gestiona los accesos a Internet pero gracias al sistema de nombres de dominio (DNS) Internet puede evolucionar y evoluciona a la velocidad que lo hace actualmente. El sistema de nombres de dominio asocia una dirección URL (nombre) con una dirección IP (una serie de números), es decir, un nombre o un número han de ser únicos. La dirección de Internet del sitio web de ICANN (www.icann.org) equivale a 192.0.34.163, o de otra forma las direcciones IP son las que utilizan los ordenadores, mientras los nombres de dominio son los que utilizan los usuarios. Eso significa que igual que no puede haber dos nombres de dominio iguales tampoco puede haber dos direcciones IP iguales. ICANN se encarga de la gestión de las direcciones IP evitando que se puedan producir repeticiones. (Pág. 35)

Sin embargo pese a que la ICANN desarrolla ciertas tareas de control e identificación en la red, la vulnerabilidad que esta brinda es que hacen falta más controles administrativos en el gobierno de internet como lo menciona Clarke (2011), si bien es cierto que la gracias a la ICANN dos dispositivos capaces de conectarse a internet no pueden tener la misma dirección IP, ya que de ser contrario, la red se confundiría entre los dos para proporcionar servicios y esto puede producir un colapso en la red, muchos expertos concuerdan en que hace falta un mayor control administrativo que regule internet y de ese modo evitar ataques cibernéticos.

En internet casi todo lo que se hace es abierto, sin codificar.

"Con el nacimiento del ciberespacio se ha difuminado el concepto de gran potencia en lo referente al "status quo" internacional tradicional, puesto que Internet es barato y tiene acceso hasta el país más pobre o cualquier persona del mundo, solo se necesita un ordenador y un hacker para poner en peligro la seguridad nacional de un país o causar graves accidentes y millones de víctimas" (Llongueras. 2013, P. 5). Si internet es de fácil acceso para cualquier persona, del mismo modo las operaciones y movimientos son totalmente abiertos, es decir sin codificación de ninguna índole. La manera más sencilla de entender ese inconveniente o vulnerabilidad en Internet, la ofrece Clarke (2011) indicando que internet es como una emisora radial de rock, esta es abierta y cualquier persona puede escuchar la música de la emisora. Según esto, solamente basta en tener un programa para capturar paquetes de información y puede mirar todo el tráfico de información que se le pueda antojar para luego copiarla o remitirla a otra página de internet.

Capacidad para propagar de forma intencional para propagar trafico malicioso diseñado para atacar los ordenadores.

Esta vulnerabilidad hace referencia a los gusanos, virus entre otros, que comúnmente se conocen como malware o software malicioso. Este software malicioso aprovecha ventajas dadas por el sistema o software, así como por los errores que pueda cometer una persona, tal como ingresar a páginas infectados o como anteriormente mencionamos, abriendo archivos adjuntos de correos que no son la entera confianza.

Este tipo de software malicioso como los virus, se transmiten bien sea a través de Internet o por medio de hardware como memorias USB que llevan la infección para obstaculizar el correcto funcionamiento de las computadoras o igualmente dispositivos electrónicos que se conecten a través de Internet, como los teléfonos inteligentes y demás para de ese modo robar información personal (Clarke et al. 2011).

Esto es una consecuencia más de la falta de control sobre Internet en el mundo, transmitiendo este tipo de software malicioso de extremo a extremo en el escenario global, dejando tanto a organismos estatales como empresario, y a la persona más normal a merced de que un hacker o ciberguerrero utilice su ordenado, información privada, y sus finanzas a su antojo.

Es una gran red con diseño descentralizado.

Jaques Bus (2011), expresa con preocupación el aumento de la ciberdelincuencia y a medida del tiempo la alta dependencia de las comunidades a medios electrónicos e Internet. "no cabe duda de que la ciberdelincuencia se está convirtiendo en un problema muy preocupante. El número de amenazas debidas a código maléfico y delictivo aumenta exponencialmente. En sólo 2008, Symantec detectó 1,6 millones de amenazas, lo que representa el 60% del total de las amenazas detectadas en todos los años anteriores a 2008" (p.17).

Según Clarke y Knake (2011), "los diseñadores de internet no querían que pudieran controlarla los gobiernos, ya fuera de forma individual o colectiva, de modo que diseñaron un sistema que otorga mucha más prioridad a la descentralización que a la seguridad" (p.118). Es de ese principio que gracias a la descentralización del sistema se logró una expansión más rápida partiendo de los objetivos de construir una red eficiente y en donde todo el mundo pudiera tener acceso y aún más importante fomentar la investigación científica. Pero aparte de generar ese éxito en el acceso por parte del general de la población, también dejó los problemas que hoy en día esa misma población debe enfrentar por falta de seguridad en sus procesos. (Clarke. Et al. 2011).

> Desde entonces y hasta la década de 1990, Internet fue considerada casi universalmente una fuerza para el bien. Pocos de los abanderados de Internet estaban dispuestos a admitir que la red era un medio neutral, a saber, que podía usarse para facilitar la comunicación libre entre los científicos y propiciar la creación de un comercio electrónico legítimo, pero que también podía

> ayudar a los terroristas a proporcionar consejos de adiestramiento a nuevos reclutas o emplearse para transmitir el video de la decapitación más reciente en la provincia de Anbar, en Irak (p.120).

Software y Hardware

Uno de los aspectos más importantes en el ciberespacio son el software y el hardware, ya que con ellos se pueden controlar los dispositivos con los cuales las personas se conectan con el ciberespacio. Y es debido a las fallas en el software y hardware que los ciberguerreros, hackers y demás pueden llegar a ocasionar daños. “El software que [estas máquinas o dispositivos] utilizan ha sido escrito principalmente por Microsoft, Oracle, IBM y Apple, pero también por muchas otras compañías. Aunque todas estas son incorporaciones estadounidenses, las maquinas (y en ocasiones el código que las controla) proviene de muchos lugares diferentes.”(Clarke et al. 2011, P. 124). En otro aparte Clarke y Knake (2011) afirman que “El software se usa como intermediario entre el usuario humano y la máquina, traduce la intención del usuario de consultar la cartelera de cine en la web o leer un blog en algo que la maquina pueda entender. Los ordenadores no son en realidad más que calculadoras evolucionadas”. (p.126)

Teniendo en cuenta la información anterior y la significativa vulnerabilidad que tienen tanto las personas, como Estados y compañías en general en el ciberespacio, se tiene que la ciberseguridad es el conjunto de políticas y acciones que se dirijan con el fin de proteger activos de una organización, y a la comunidad en general en el ciberespacio (UIT. 2014); en cuanto a ciberdefensa, esta se cataloga como las actividades o procedimientos dirigidos a preservar la seguridad de los sistemas de información ya sea de una organización o a las personas de una comunidad (Zea. 2013).

En el siguiente capítulo, se describirán los más importantes ataques informáticos contra los Naciones y sus consecuencias en el orden mundial; países que poco a poco voltean a ver el tema de la ciberseguridad y ciberdefensa con ojos diferentes luego de dichos hechos.

CAPITULO 2

DE LA TEORIA A LA PRÁCTICA: LOS MÁS SONADOS ATAQUES CIBERNETICOS PROPINADOS A LOS ESTADOS Y SUS ESTRATEGIAS PARA MITIGARLOS.

Uno de los casos más recordados es el que tiene que ver con el ataque por parte de los rusos a Estonia. El diario El País de España (2009), realiza una breve descripción de los hechos (ver anexos), señalando que por la implicación política que tienen ciertos símbolos rusos que recuerdan la liberación de los países antes miembros de la Unión de Repúblicas Socialistas Soviéticas (URSS) la las garras de los nazis de Hitler durante la Segunda Guerra Mundial, y que están presentes en los países de la llamada Cortina de Hierro, fueron el foco para que los hackers rusos, con ayuda del gobierno (Clarke et al. 2011) realizaran una serie de acciones por medio de ataques distribuidos de denegación de servicio (DDOS) que anteriormente se ha descrito en el capítulo número uno. Clarke hace una clase de "descripción forense" acerca de lo que ocurrió aquel día en Estonia y relaciona los conceptos que se repasaron en la anterior sección.

> *[…] El DDOS dirigido contra Estonia fue el más grande nunca visto hasta entonces. Todo indica que en el ataque participaron varias botnets diferentes, cada una de las cuales contaban con decenas de miles de máquinas infectadas que hasta ese momento habían estado dormidas. En un primer momento, los estonios pensaron que la caída de algunas de sus páginas web no era más que una molestia obra de un puñado de rusos indignados. Luego, sin embargo, las botnets empezaron a atacar direcciones de Internet desconocidas para la mayoría de las personas, a saber, no las de sitios web públicos, sino las de los servidores que se ocupan de ciertas partes de la red telefónica, el sistema de verificación de las tarjetas de crédito y el directorio de Internet. Para entonces más de un millón de ordenadores participaban en la avalancha de solicitudes de conexión que inundó los servidores elegidos como blanco. El Hansapank, el banco más grande del país, se tambaleo. A lo largo y ancho del país, el comercio y las comunicaciones se vieron afectados. Y los ataques no se detuvieron ahí.*
>
> *En la mayoría de ataques DDOS previos, se golpeaba a un sitio durante unos cuantos días. El ataque contra Estonia fue algo diferente. Centenares de sitios claves en un solo país fueron atacados durante semana tras semana, sin tiempo para recuperarse […]. (Pág. 34)*

Las investigaciones por parte de los organismos de control como la OTAN, arrojaron que los ordenadores zombis contactaban sus controladores que estaban localizados en Rusia. Los rusos nunca aceptaron el ataque y se escudaron en aquellos patriotas que poseían ese tipo de conocimiento; pero como lo afirma Clarke (2011, P. 36), "al crimen organizado se la ha permitido prosperar debido a sus vínculos no reconocidos con los servicios de seguridad" (rusos).

Tras este ataque, la OTAN adelanto gestiones para crear un centro especializado en ciberdefensa, y de este modo, prevenir posibles ataques futuros. Sin embargo, estos esfuerzos serían infructuosos luego de un nuevo ataque por parte de Rusia; esta vez durante el enfrentamiento militar sostenido con otra población soviética. Sería el turno para el ataque contra Georgia en 2008 (El País. 2008). Esta es la primera vez en que se mezcla un ciberataque al mismo tiempo de una confrontación bélica.

Si se indaga más acerca de ataques informáticos se puede evidenciar que se presentan más casos como el ataque de Israel a Siria en 2007, en el cual se neutralizaron todos los sistemas antiaéreos de Siria para poder bombardear una presunta planta nuclear que se construía con cooperación de Corea del Norte, o también el ataque a varias páginas del gobierno de Estados Unidos por parte de ciberguerreros de Corea del Norte (Clarke et al. 2011 P. 17 - 56).

Como quiera, es notorio que el ciberespacio, como lo anota Joyanes (2011), ha sido declarado por prestigiosos expertos e investigadores como el quinto dominio después de la tierra el aire, el mar y el espacio. Es importante mencionar que países que no son bélicamente simétricos con las grandes potencias, han descubierto en el ciberespacio el escenario propicio para hacer menor ese tipo de asimetrías a la hora de una confrontación bélica. De los hechos descritos anteriormente fácilmente se puede deducir que un país bélicamente débil puede comenzar una confrontación atacando infraestructura crítica del poder duro sin la necesidad de disparar una sola bala. Por ejemplo podría atacar las compañías eléctricas insertando bombas lógicas en los sistemas SCADA (Supervisory Control and Data Acquisition) que según describe

Clarke (2011) “son programas de software y la mayoría de las compañías eléctricas usa uno de la media docena de productos disponibles en el mercado” (p.139). Vale la pena aclarar, que no solo las redes eléctricas funcionan con este tipo de software. Según Joyanes (2011), estos sistemas SCADA son utilizados por gran mayoría de plantas industriales y de todos los ramos. A su vez, estos sistemas día tras día aumentan vertiginosamente su conexión a Internet, lo que aumenta “el riesgo de sufrir ataques remotos.

Describe igualmente, que este tipo de programas funcionan enviando señales a través de redes internas que según estudios, muchas de esas redes internas o Intranet, se encuentra al mismo tiempo conectadas a redes públicas (Clarke.2011). Pero, como se anotó anteriormente, una de las vulnerabilidades del software es que pueden crearse puertas traseras para realizar cambios en el sistema. Claramente, desconectado la energía eléctrica, muchos de los sistemas de defensa depende de este servicio y de manera inmediata quedarían neutralizados. Este sería solamente un ejemplo de qué redes o puntos estratégicos podrían vulnerarse. Es claro que si se recuerda el escenario del comienzo de este trabajo, que los sistemas de transporte, servicios públicos, y todo medio que se encuentre altamente dependiente a Internet o a una red informática será blancos predilectos para un ataque.

Un aspecto que ha hecho presencia en este escenario es Internet móvil, el cual mediante un teléfono inteligente o una tableta electrónica en primera instancia es utilizada como una herramienta de negocio que optimiza el tiempo de las personas aparte de ofrecer todo tipo de aplicaciones de uso normal por parte de las personas del común, lo que hace que la dependencia a Internet sea mayor con el pasar de los días. Cualquier tipo de dispositivo que tenga la capacidad de ingresar al ciberespacio es un potencial blanco para ser un botnets o llevar consigo virus informático.

Este tipo de dispositivos se encuentran a una seria de servidores que configuran la llamada “nube”. Frente a ello, Llongueras (2011) realiza una descripción de la nube o *cloud computing.*

> (…) es un paradigma en el que la información se almacena de manera permanente en servidores de Internet y se envía a cachés temporales de cliente; es un nuevo modelo de prestación de

> servicios de negocio y tecnología, que permite al usuario acceder a un catálogo de servicios estandarizados y responder a las necesidades del negocio, de forma flexible y adaptativa, en caso de demandas no previsibles o de picos de trabajo, pagando únicamente por el consumo efectuado. Esta tecnología pasará a ser parte esencial de la economía y de la sociedad en general pero nos plantea los problemas siguientes: ciberespionaje, venta de datos privados, seguridad de estos servicios externalizados. (Pág. 20)

Frente a ello, las grandes potencias y otros países interesados en proteger sus sistemas, o que están interesados en el ciberespacio para tomar una ventaja competitiva, han ahondado esfuerzos para crear instituciones altamente capacitadas para contrarrestar estas amenazas latentes, teniendo en cuenta el principio de tener un buen ciberarsenal, sin descuidar las cuestiones de defensa contra este tipo de ataques.

Si bien es cierto que en una guerra convencional se busca no afectar a la población civil, "El uso de ciberarmas contra las infraestructuras de una nación inevitablemente se traduciría en un ataque contra los sistemas civiles" (Clarke et al. 2011, P. 314). Por esta razón muchos expertos concuerdan en que es necesario realizar acuerdos y más legislación internacional en torno a combatir el cibercrimen y regular los Sistemas de Información y comunicaciones. A continuación se hará una breve descripción de las estrategias que algunos países están tomando en cuenta para sus políticas de ciberseguridad y ciberdefensa.

La estrategia de Estados Unidos

Llongueras indica que "La ciberseguridad no es exclusivamente un problema militar aunque los conceptos y el lenguaje utilizado en este ámbito son igualmente una derivación de los conceptos utilizados tradicionalmente en el ejército: amenaza, agresión, ataque, defensa son los términos más utilizados. Pero la ciberseguridad es un desafío para la sociedad como un todo y necesita una respuesta que surja de la cooperación entre los diversos actores." (2013, P. 26).

De acuerdo con esto los Estados Unidos tienen una capacidad muy limitada para contener un ciberataque según lo afirma el ex asesor presidencial Richard Clarke (2011), dado que se han centrado más en la capacidad de ataque que en la defensa por motivo de la interpretación que la mejor defensa es el ataque, sin embargo, ¿Qué tan efectivo es atacar primero si no se va a saber quién y en dónde se va a presentar un contraataque?

Jordi molas (2007) realiza un resumen sobre las actividades que adelanta Estados Unidos en materia de ciberdefensa.

> El volumen de investigación militar realizado en los EE.UU. es muy superior al que realizan todos los países europeos juntos. La inversión en I+D realizada por el Pentágono y otros departamentos, como el de Energía, con responsabilidades en el campo de la defensa y las infraestructuras que los apoyan no pueden compararse al ámbito europeo, donde las inversiones son mucho menores y se encuentran repartidas entre varios países. Esta sección discute brevemente las actividades de la "Defense Advanced Research Projects Agency" (DARPA), una organización que por sus peculiaridades y sus éxitos ha sido presentada a menudo como un ejemplo a seguir por una posible agencia europea de investigación. Sin embargo, DARPA debe entenderse como una parte relativamente pequeña del amplio sistema de innovación militar norteamericano. (Pág. 81)

De acuerdo con Clarke (2011), cada una de las instituciones encargada de la seguridad del país, (Marina, Fuerza Aérea, especialmente) abrió su propio departamento especializado en la ciberguerra luego de la creación del Cibermando de Estados Unidos en 2009. Teniendo en cuenta que había personal partidario de crear un mando unificado para esta tarea, el mando espacial se unió con el Mando Estratégico o STRATCOM, y este pasó a ser responsable de centralizar los recursos para la ciberguerra. Sin embargo se presentarían rencillas internas puesto que la Fuerza Aérea quería el ostentar el dominio de cualquier actividad que tuviera que ver con la defensa del ciberespacio estadounidense. Se definió entonces que todos los servicios harían parte del mando central, incluyendo a la CIA, la NSA y otros organismos de inteligencia norteamericanos.

Para el estamento militar estadounidense en general ha recalado la idea que el ciberespacio es algo que hay que dominar para evitar acciones por parte de países potencialmente enemigos (Clarke et al. 2011). Sin embargo, solamente se centran en la necesidad de atacar a otras naciones primero, pero no se han centrado en una real defensa de sus instalaciones tanto civiles como militares.

Actualmente, Estados Unidos se encuentra enfrascado en una seria de acusaciones por parte de ambas naciones, en donde dicen ser mutuamente espiados cibernéticamente según el portal de noticias Voz de América (2014). Con esto el jefe del Pentágono, Chuck Hagel, afirma que para 2016 tendrá en el cibermando a más de seis mil especialistas para contrarrestar cualquier tipo de ataque sobre los Estados Unidos, al mismo tiempo que afirma que para la administración Obama es una prioridad proteger el ciberespacio de piratas informáticos, teniendo en cuenta la dependencia significativa de este país hacia el ciberespacio. Sin embargo Según Clarke (2011) Estados Unidos sigue centrándose en atacar o sabotear a otras naciones antes que concentrarse en la defensa de sus estructuras, lo cual puede incrementar el nivel de sensibilidad en caso de un ataque, en lo cual se está trabajando comenzando por la sensibilización a las personas en cuanto a seguridad de la información se refiere.

Según Javier Candau (2011), Estados Unidos centra sus esfuerzos en 5 aspectos principales a saber:

1. **Sistema de respuesta nacional de seguridad en el ciberespacio**.
2. **Programa de reducción de amenazas y vulnerabilidades**.
3. **Formación y concienciación en el ciberespacio**.
4. **Asegurar el ciberespacio gubernamental**.
5. **Cooperación nacional e internacional.**

Unión Europea y OTAN

Pastor, Pérez, Arnaíz & Toboso (2009) dan a conocer los pasos que han venido dando tanto la Unión Europea y la OTAN en cuando a ciberseguridad y ciberdefensa en el ámbito de políticas y otras medidas tomadas para hacer del su ciberespacio algo más seguro. En la unión Europea se hace enfoque en la preservación de las estructuras Críticas, y dentro de estas infraestructuras críticas se incluyen las Tecnologías de Información.

Ellos plantean que estos esfuerzos se ven materializados en la creación de organizaciones y programas especializados en el cuidado de estas estructuras Críticas, como el Programa Europeo para la Protección de las Infraestructuras Críticas (PEPIC) y la Red de Alerta en relación con las Infraestructuras Críticas (CIWIN). Así mismo, se plantea la importancia de la lucha contra los delitos informáticos como la Decisión Marco 2005/222 sobre "ataques contra los sistemas de información".

Sobre la OTAN Pastor, Perez Arnaiz y Toboso (2009) indican:

> Los principales esfuerzos realizados por la OTAN en Ciberdefensa son los siguientes:
> • Creación de un Centro de respuesta ante incidentes de seguridad informática, el NCIRC (NATO Computer Incident Response Capability) en el año 2004.
> • Aprobación de la Política de Seguridad en Ciberdefensa de la OTAN ("Nato Policy on Cyber Defense") el 7 de Enero del 2008.
> • Acuerdo sobre el "Concepto de Ciberdefensa de la OTAN" ("NATO Cyber Defence Concept") a comienzos del año 2008.
> • Asignación de las Responsabilidades en Ciberdefensa, y creación de las nuevas estructuras organizativas necesarias para la implementación de la Política de Ciberdefensa, entre las que destacan:
>
> - La Autoridad de Gestión de la Ciberdefensa de la OTAN (NATO Cyber Defence Management Authority, NCDMA) creada en el 2008.
> - El Centro de Excelencia Cooperativa de Ciberdefensa (Cooperative Cyber Defence Centre of Excellence, CCD COE) creado también en el 2008. (Pág. 35)

China

Según Clarke y Knake (2011, P. 77), los chinos fueron los más interesados en saber lo que pasaba durante el desarrollo de la operación Tormenta del Desierto en el Golfo Pérsico para evaluar en qué nivel se encontraban en caso de afrontar una guerra con Estados Unidos. Fue tan notoria la asimetría en cuanto a poder bélico, que optaron por encontrar otro tipo de mecanismo para poder llegar de igual a igual a los norteamericanos. Redujeron el tamaño de su ejército y con ello invirtieron en nuevas tecnologías e investigación.

Los oficiales chinos tenían la idea de que quien tiene la información tendrá el poder y que la información podría tenerse mediante un ataque cibernético preventivo (Clarke et al. 2011, P. 78). Según estudios realizados "Hay datos que hacen pensar que el gobierno chino deriva fondos para financiar la comunidad *hacker*. Por otra parte, los servicios de inteligencia chinos continuamente realizan estudios sobre ciencia y tecnología para ayudar a conseguir los objetivos nacionales. China fabrica productos relacionados con las TIC para conocer sus necesidades tecnológicas. Además de cooperar con Rusia, un país donde también existe un programa de ciberguerra, se sospecha que China tiene su propio modelo de uso de las tecnologías en ciberataques (Pastor et al. 2009, P. 126)

Es claro que los estadounidense, como potencia tecnológica, ve con preocupación este tipo de avances, según ellos, china ha estado trabajando en algunos aspectos desde los la década de los 90. Esos aspectos son crear grupos de hackers civiles, emprender amplias labores de ciberespionaje, incluso de software y hardware estadounidense, adoptar varias medidas para defender su propio ciberespacio, establecer unidades militares para la ciberguerra y plantar bombas lógicas en las infraestructuras estadounidenses (Clarke et al. 2011, P. 84). Es esta la razón por la que en los últimos meses se acusan mutuamente de realizar ciberespionaje, lo que desata algunas tensiones en el ambiente político y tecnológico.

Rusia

Como se ha visto al comienzo de este capítulo, los rusos tienen un gran poder para realizar un ataque cibernético, como los casos presentados en Estonia y en Georgia. Se denota un *modus operandi* en el que los rusos buscan bloquear en los campos más significativos a sus potenciales enemigos, dejándolos totalmente incomunicados, sin acceso a su dinero y bloqueando sus páginas estatales. El programa Ruso describe el momento exacto para atacar, luego de tener penamente identificados los objetivos, tales como los nombrados anteriormente y añadiéndole el componente de operaciones psicológico y desinformando totalmente a las personas (Pastor et al. 2009, P. 124). Como se estudió en los incidentes con Georgia y realizando una pequeña comparación con el programa estadounidense, la gran ventaja que tiene Rusia es que posee mecanismos más eficaces de defensa que los estados unidos, como se pudo apreciar en el caso con Georgia, en donde los georgianos intentaron contrarrestar el ataque, pero los rusos pudieron neutralizar totalmente cualquier intento de los georgianos.

Los rusos conservan una postura aparentemente neutral en cuanto a la aplicación de la ciberguerra. Consideran que cada estado está en la libertad de proteger los flujos de información de la manera como sus investigaciones avancen y los frutos que estas mismas den (Pastor et al. 2009, P. 124).

En este capítulo se observa que los programas para evitar o enfrentar la ciberguerra necesitan de conocer las capacidades y debilidades a las que un Estado puede estar expuesto, los niveles de sensibilidad y vulnerabilidad a la hora tanto de atacar como de defender, el impulso de la investigación científica para proteger los flujos de información de ataques cibernéticos y, naturalmente, conocer las capacidades de potenciales enemigos para estar preparados y defender tanto redes estatales, como infraestructura critica que pueda vulnerar el bienestar de la población civil.

Para ello es muy importante la inversión que se realice a este tipo de programas de ciberseguridad y ciberdefensa, darle la importancia que merece el tema y no dejar nada al azar,

porque en el momento menos pensado, tanto estados como grupos interesados en debilitar el poder del estado, sea cual fuere la razón, puede vulnerar todo el sistema de una país y no solamente causar la perdida de información, dinero, comunicación, sino lo más importante desatar caos en la población y provocar pérdida de miles de vidas.

Es importante que la capacidad de disuasión de un estado sea óptima, ese es el primer paso para evitar una escalada en cualquier tipo de conflicto, incluyendo la ciberguerra. Sobre ello, Llongueras (2013), indica

> La dificultad de control de lo que sucede en Internet hace necesario crear un plan de ciberdisuasión como arma efectiva y elemento fundamental de la ciberdefensa y de la estrategia militar. Para que la disuasión sea efectiva los antagonistas, enemigos o futuros atacantes deben estar convencidos que pueden ser identificados, perseguidos y castigados severamente. (p.27)

Queda claro entonces, que para poder tener poder de disuasión en el ciberespacio se necesita invertir en mecanismos para poder identificar la fuente de los ataques, así como poder de ataque y defensa.

CAPITULO 3

¿CÓMO ESTÁ COLOMBIA EN MATERIA DE CIBERSEGURIDAD Y CIBERDEFENSA?

Según estudios realizados por el Ministerio de Defensa Nacional de Colombia, a través de la Dirección de Estudios Sectoriales (2009), "para el año 2000 tan solo el 2% de la población tenía acceso a Internet; actualmente el 40% hace uso constante de este medio (Figura1), ubicando al país en el cuarto lugar en el ranking de usuarios de América Latina (Figura2) y en el puesto 24 del mundo."

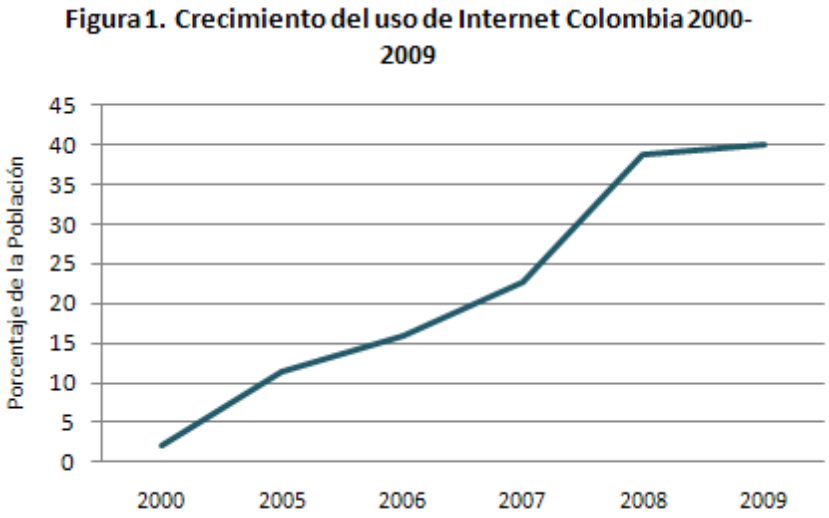

Figura 1 Crecimiento del uso de Internet Colombia 2000-2009

Fuente: Ministerio de Defensa Nacional de Colombia

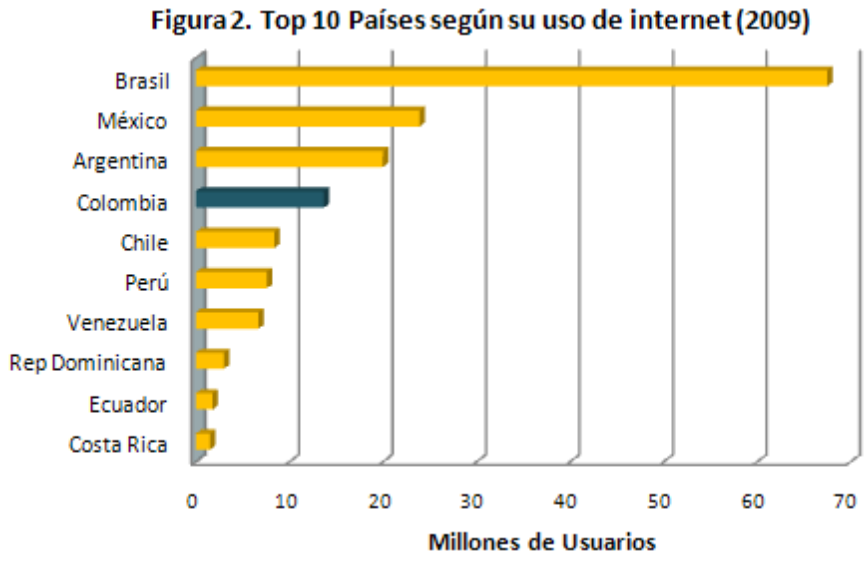

Figura 2 Top 10 Países según su uso de Internet (2009)

Fuente: Ministerio de Defensa Nacional de Colombia

Según este estudio realizado, Colombia ha enfrentado numerosos ataques informáticos a páginas oficiales del gobierno como la página de la presidencia de la República, Gobierno en línea, Ministerio del Interior y de Justicia, Defensa y Cultura, los cuales dejaron estas páginas fuera de servicio por varias horas (Departamento Nacional de Planeación, 2011, P.9), y del mismo modo la Policía Nacional ha reportado casos como robo de identidad, robo a cuentas bancarias que a 2009 llegaban a 50.000.000 millones de dólares (Ministerio de Defensa, 2009, p.1). Del mismo modo intento atentarse contra la infraestructura crítica de la nación, pero estos fueron repelidos. Sin embargo, los organismos de seguridad colombianos son conscientes del hecho que el nivel de sofisticación de los ataques va en aumento y es necesario tener en cuenta ello para evitar problemas en el futuro.

Desde el año 2005 se creó un grupo interagencial liderado por el Ministerio de Relaciones Exteriores, en conjunto don el Ministerio del interior y de Justicia, el Ministerio de Defensa Nacional y posteriormente el Ministerios de las Tecnologías de la Información y las Telecomunicaciones (TIC's) y Entidades relacionadas con este tema, decidieron que quien

levaría las riendas de la ciberseguridad y la ciberdefensa de Colombia seria el Ministerio de Defensa Nacional. (Ministerio de Defensa, 2009, P. 4)

De este trabajo mancomunado entre las instituciones anteriormente relacionadas se gesta en 2009 el ColCERT (Equipo de Respuesta a Emergencias Informáticas de Colombia), "cuya función principal es la de coordinar las acciones necesarias para la protección de la infraestructura crítica del Estado colombiano, frente a emergencias cibernéticas que atenten o comprometan la Seguridad y Defensa Nacional" (Ministerio de Defensa, 2009, P.4). De acuerdo con este informe el trabajo va en caminado en tres ejes temáticos principales.

En primera instancia se enfoca en el fortalecimiento jurídico e institucional, el cual se refiere a adopción y adaptación del sistema de legislativo y judicial para los temas de ciberseguridad. En segundo término plantea los asuntos internacionales como plano de vital importancia para los intereses colombianos, esto se traduce en una misión de observación de los casos internacionales y que tendencias se marcan en el ámbito de la ciberseguridad y ciberdefensa en cuanto a medidas a preventivas que lleven a una minimización del riesgo de sufrir ataques cibernéticos, así como implementación de acuerdos sobre la materia que pueda asumir el estado ya sea bilateral o multilateralmente. En tercer lugar se encuentran las medidas contra el delito cibernético. Con ello se refieren a las capacidades que puede adquirir en cuanto a sistemas de defensa que mediante el ColCERT se ponen en marcha para mitigar potenciales ataques (Ministerio de Defensa, 2009, P. 4). En cuanto al ColCERT, se enfatiza que es importante trabajar de mano de las entidades privadas para obtener financiación y de ese modo se pueda evolucionar en el fortalecimiento de esta entidad y que no quede como un proyecto inconcluso.

En la actualidad esta entidad a través de su página en Internet www.colcert.gov.co, brinda información acerca de foros mundiales sobre seguridad informática, así como asesorías y actualizaciones de seguridad para sistemas operativos y de ese modo reducir la vulnerabilidad de los ordenadores (Ver Figura 3 y 4).

Figura 3 Portal Web ColCERT, www.colcert.gov.co. Autoría Propia

Figura 4 Sección de información acerca de boletines de seguridad, Eventos y actualizaciones de seguridad para sistemas Operativos www.colcert.gov.co. Autoría propia.

Así mismo, el Consejo Nacional de Política económica Y social del Departamento Nacional de Planeación (DNP), emitió en 2011 un documento CONPES Sobre los lineamientos de política para ciberseguridad y ciberdefensa con colaboración de todas las instituciones que tienen que ver con este tema, como el Ministerio de Defensa, Ministerio de Interior, Ministerio de TIC's entre otras (2011).

En este documento se explica cómo se ha venido tratando el tema en el país, con el acompañamiento de organizaciones como la OEA ha venido organizando talleres y seminarios sobre la materia de ciberseguridad y ciberdefensa, así como la creación de mecanismos y estrategias que permitan la lucha frontal contra la criminalidad cibernética y la protección de infraestructuras críticas que puedan ser objeto de ataques cibernéticos. (DNP, 2011)

Del mismo modo, este documento da a conocer las distintas leyes e iniciativas que el gobierno ha impulsado desde tiempo atrás para mejorar la calidad de la utilización del ciberespacio en Colombia, entre ella se destacan las siguientes (DNP, 2011, P.11):

- Ley 527 de 1999 - COMERCIO ELECTRÓNICO Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones"

- Ley 599 DE 2000 Por la cual se expide el Código Penal. En esta se mantuvo la estructura del tipo penal de "violación ilícita de comunicaciones", se creó el bien jurídico de los derechos de autor y se incorporaron algunas conductas relacionadas indirectamente con el delito informático, tales como el ofrecimiento, venta o compra de instrumento apto para interceptar la comunicación privada entre personas. Se tipificó el "Acceso abusivo a un sistema informático", así: "Art. 195. El que abusivamente se introduzca en un sistema informático protegido con medida de seguridad o se mantenga contra la voluntad de quien tiene derecho a excluirlo, incurrirá en multa."

- Ley 962 de 2005 Por la cual se dictan disposiciones sobre racionalización de trámites y procedimientos administrativos de los organismos y entidades del Estado y de los particulares que ejercen funciones públicas o prestan servicios públicos.

- Ley 1273 de 2009 Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

- Ley 1341 de 2009 Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las tecnologías de la Información y las Comunicaciones –TIC, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones.

- Circular 052 de 2007 (Superintendencia Financiera de Colombia).

Aparte de este ordenamiento jurídico interno que el mismo Conpes califica como insuficiente, se tienen instrumentos e iniciativas dentro del marco internacional como (DNP, 2011, P 14 – 15):

- Convenio sobre Ciberdelincuencia del Consejo de Europa – CCC (conocido como el convenio sobre cibercriminalidad de Budapest) Adoptado en noviembre de 2001 y entrada en vigor desde el 1° de julio de 2004.

- Resolución AG/RES 2004 (XXXIV-O/04) de la Asamblea General de la Organización de los Estados Americanos. Estrategia Integral para combatir las amenazas a la seguridad cibernética: Un enfoque multidimensional y multidisciplinario para la creación de una cultura de la seguridad cibernética. Estipula tres vías de acción:

- Creación de una Red Hemisférica de Equipos Nacionales de Respuesta a Incidentes de Seguridad de Computadores - CSIRT16.
- Identificación y adopción de normas técnicas para una arquitectura segura de Internet.
- Adopción y/o adecuación de los instrumentos jurídicos necesarios para proteger a los usuarios de Internet y las redes de información de los delincuentes y los grupos delictivos organizados que utilizan estos medios, a cargo de las Reuniones de Ministros de Justicia o de Ministros o Procuradores Generales de las Américas - REMJA.

- Consenso en materia de ciberseguridad17 de la Unión Internacional de Telecomunicaciones - UIT, en el seno de Naciones Unidas, en desarrollo del programa de acciones de Túnez para la sociedad de la información de 2005.
- Resolución 64/25 "Los avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional" Asamblea General de las Naciones Unidas. (2009)

El objetivo primordial de este documento es "Fortalecer las capacidades del Estado para enfrentar las amenazas que atentan contra su seguridad y defensa en el ámbito cibernético (ciberseguridad y ciberdefensa), creando el ambiente y las condiciones necesarias para brindar protección en el ciberespacio" (DNP, 2011, P. 21). Para ello se propone organizar la comisión intersectorial que se mencionaba en el primer informe del Ministerio de Defensa (2009) junto con la operación del ColCERT, como lo muestran las figuras 5 y 6

Figura 5 **Modelo de Coordinación**

Fuente: Ministerio de Defensa Nacional

Figura 6 **Modelo Relacional del ColCERT**

Fuente: Ministerio de Defensa Nacional

Es de este modo en que se presenta el plan para institucionalizar el método de ciberseguridad y ciberdefensa de Colombia mediante un modelo de cooperación interinstitucional, acompañado claramente del sector privado y el componente primario para que este proyecto se dé paulatinamente como es la academia, a través de sus centros de investigaciones, así como otros CSIRTs (Computer Security Incident Response Team, Equipo de Respuesta ante Incidencias de Seguridad) los comandes cibernéticos tanto policiales como conjuntos con las otras fuerzas armadas colombianas.

CONCLUSIONES

Las tecnologías de información y telecomunicaciones van avanzando a un ritmo más rápido al pasar de los días. Por ello, es importante estar a la vanguardia de los mecanismos para salvaguardar no solo la información sensible de los pobladores de un país o el ataque a una página oficial que se cataloga como un ataque de baja intensidad, sino también tener sistemas de defensa que permitan proteger las infraestructuras críticas que con el paso del tiempo son más dependientes del ciberespacio y si no se protegen la sociedad estaría presenciando un ataque de alta intensidad.

Teniendo en cuenta la vulnerabilidad que presenta el ciberespacio, aún hace falta mayor cooperación internacional para construir una verdadera administración de este dominio, dado que a pesar que las potencias mundiales son fuertes bélicamente y poseen ejércitos a la vanguardia en armamento cinético, las asimetrías de poder se hacen menos notorias en el mundo cibernético. Con lo cual se hacen igual de vulnerables que si no tuvieran armamento avanzado, añadiendo a esto que el siguiente movimiento de un adversario la red es impredecible. Nunca se va a conocer en donde será el siguiente ataque. Los bloques económicos y comunidades regionales han realizado esfuerzos por controlar y regular en su medida la red, sin embargo se deben propender por adaptar medidas más eficaces para mitigar al máximo un ciberataque.

El campo de la investigación acerca del ciberespacio para diseñar políticas para la ciberseguridad y ciberdefensa ha sido importante en los últimos tiempos. Razón por la cual, es importante fomentar la investigación entre los estudiantes, no solo en el área tecnológica. El área política, del derecho y la mayoría de ramas de estudio deben trabajar conjuntamente al igual que las instituciones estatales para en verdad lograr estar a la vanguardia sobre las tecnologías de la información y llegar a innovar en este escenario.

Dentro de una confrontación convencional normalmente se vela por excluir al personal civil de esta. Sin embargo, con los ataques cibernéticos es prácticamente inevitable pensar que la población civil no va a resultar afectada, es este campo de batalla virtual, que a la hora de la

verdad resulta ser más real de lo esperado, no distingue entre instalaciones militares y servicios vitales para la población, lo cual, provocaría un cataclismo de dimensiones incalculables. Es por esta razón que es importante la capacidad de ataque, pero muchos más la capacidad de defensa para de este modo minimizar la sensibilidad a la hora de recibir un ataque contra infraestructuras críticas y otro tipo de objetivos que se pueden afectar con un ataque cibernético.

Al atacar infraestructuras críticas no solo se pone a prueba el mando militar u organizaciones estatales, las instituciones de carácter privado también son afectadas, tales como banco, proveedores de servicios públicos y transportes. Esto quiere decir, que la seguridad y defensa del ciberespacio tiene implicaciones civiles y económicas y esto lo convierte en un objetivo estratégico de la seguridad nacional, por lo tanto los hombres y mujeres que ostentan tal responsabilidad deben estar intelectualmente preparados para asumir el compromiso de la defensa de un país en el teatro de operaciones del ciberespacio.

Las ciberarmas deben controlarse. De lo contrario, como se observó en los casos de ataques rusos, cualquier tensión diplomática podría convertirse en un ataque informático que produciría una escalada en el conflicto, que desbordaría en una confrontación armada regular. A pesar de que en un ciberataque no se dispara una sola bala, el caos que generaría podría ser desastroso para cualquier país que sufra este tipo de agresión. Hoy en día si se comete un crimen a través del ciberespacio es muy complicado hacer justicia, dado que como muchos expertos afirman, el ciberespacio se está convirtiendo en el arma perfecta, por esto la necesidad al mismo tiempo de controlar las ciberarmas, de acabar con el cibercrimen.

Colombia busca ponerse a la vanguardia en su región en cuanto a ciberseguridad y ciberdefensa se refiere. Desde hace aproximadamente 15 años viene adelantando gestiones para proteger la información sensible de la población, sin embargo el gobierno es consciente que debe trabajar profundamente en la creación de estamentos e instituciones que permitan controlar aún más los delitos informáticos y ciberataques a su infraestructura crítica. Por esa razón, es muy útil el esfuerzo de crear unidades militares de policía con las que actualmente ya se cuenta, al igual que una agencia que prevenga cualquier clase de delitos informáticos, con el fin de mantener

informada a la población de cualquier tipo de amenaza, ya que si este tipo de información se mantiene bajo reserva, cualquier esfuerzo por evitar un ciberataque será infructuoso.

A medida que se crean distintos modos d conectividad en la red, deben crearse los correspondientes mecanismos de protección para evitar que los dispositivos sean infectados con diversos virus, o aplicaciones y programas que puedan hacer de un teléfono inteligente, Tablet o cualquier otro equipo en atacante de otra red. Muchas veces se pensó que la guerra en el ciberespacio era la guerra del futuro. Valdría la pena reevaluar esa afirmación y pensar si el mundo está viviendo la guerra cibernética en este preciso instante.

REFERENCIAS

Instituto Español de Estudios Estratégicos, Instituto Universitario "General Gutiérrez Mellado" (2011) *Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio*. Madrid (Esp.) Ministerio de Defensa Español.

Unión Internacional de Telecomunicaciones ITU (2007) *Guía de Ciberseguridad para los países en Desarrollo.* Recuperado de www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2007-MSW-S.doc

BBC Mundo. 2013. Lo que Snowden ha revelado hasta ahora del espionaje de EE.UU. Extraído febrero 2 2014, desde

http://www.bbc.co.uk/mundo/noticias/2013/07/130702_eeuu_snowden_revelaciones_espionaje_wbm.shtml

Actualidades de la UIT. Extraído en marzo 2014 desde http://www.itu.int/net/itunews/issues/2010/09/20-es.aspx

Clarke, R. & Knake, R. (2011). *Guerra en la red, los nuevos campos de batalla.* Barcelona. Editorial Planeta.

Caro, M. (2011). *Alcance y ámbito de la seguridad nacional en el ciberespacio.* Para Instituto Español de Estudios Estratégicos, Instituto Universitario "General Gutiérrez Mellado" (2011) Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio. Madrid (Esp.) Ministerio de Defensa Español.

Llongueras, A. (2013). *La guerra inexistente, la ciberguerra.* Madrid (Esp.). Eae Editorial Acad MIA Espa Ola.

Acosta, O. Pérez, J. Arnáiz, D. & Taboso, P. (2009). *Seguridad Nacional y Ciberdefensa.* Madrid (Esp.). Fundación Rogelio Segovia para el Desarrollo de las Telecomunicaciones.

Clarke, R. Knake R. (2011) Ensayos. En Clarke, R. & Knake, R. Guerra en la red: Los nuevos campos de batalla (P. 17 – 56). Barcelona. Editorial Planeta.

Actualidades de la UIT. Extraído en marzo 2014 desde http://www.itu.int/net/itunews/issues/2010/09/20-es.aspx

Las Fuerzas Armadas se preparan para afrontar con éxito los nuevos retos del siglo XXI en materia de ciberseguridad, ciberdefensa militar. Extraído en febrero de 2014 desde http://www.emad.mde.es/DOCUMENTOS-INTERES/multimedia/documentos-descargados/documentosEMAD/130301-CIBERDEFENSA_-RED.pdf

Bus, J. (2011) *Dependencia y confianza social.* Para Unión Internacional de Telecomunicaciones (2011). La búsqueda de la paz en el ciberespacio. Ginebra. ITU.

Estonia, primera víctima de los hackers. Extraído en marzo 2014 desde http://elpais.com/diario/2009/05/30/internacional/1243634402_850215.html

Georgia sufre la guerra cibernética. Extraído en marzo 2014 desde http://elpais.com/diario/2008/08/14/internacional/1218664803_850215.html

Joyanes, L. (2011) *Introducción. Estado del arte de la ciberseguridad.* Para Instituto Español de Estudios Estratégicos, Instituto Universitario "General Gutiérrez Mellado" (2011) Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio. Madrid (Esp.) Ministerio de Defensa Español.

Molas, J. (2007) *Políticas de I+D de Defensa de varios países europeos y de EE.UU*. En *Relaciones entre las innovaciones tecnológicas y la Defensa*. Madrid (Esp.) Fundación Rogelio Segovia Para el Desarrollo de las Telecomunicaciones.

Candau, J. (2011). *Estrategias Nacionales de Ciberseguridad. Ciberterrorismo.* Para Instituto Español de Estudios Estratégicos, Instituto Universitario "General Gutiérrez Mellado" (2011) Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio. Madrid (Esp.) Ministerio de Defensa Español.

EE.UU se prepara para la ciberguerra. Extraído en marzo 2014 desde http://www.voanoticias.com/content/eeuu_internet_ciberguerra_militar/1882151.html

Pastor, O. Pérez, J. Arnaíz, D. & Taboso, P. (2009). *Seguridad Nacional y ciberdefensa*. Madrid (Esp.). Fundación Rogelio Segovia Para el Desarrollo de las Telecomunicaciones.

Ciberseguridad y Ciberdefensa: Una primera Aproximación. Extraído en Julio de 2013 desde http://www.mindefensa.gov.co/irj/go/km/docs/Mindefensa/Documentos/descargas/estudios%20sectoriales/Notas%20de%20Investigacion/Ciberseguridad%20y%20ciberdefensa.pdf

Departamento Nacional de Planeación. *Documento Conpes 3701, Lineamientos de Política Para Ciberseguridad y Ciberdefensa.* Bogotá D.C., 14 de julio de 2011