INCIDENCIA DE LAS AGRESIONES A LA SEGURIDAD CIBERNÉTICA EN EL DESARROLLO INFORMÁTICO DE LAS FUERZAS ARMADAS DE ESTADOS UNIDOS (2003-2013)

NICOLE VANESSA TORRES VARGAS

UNIVERSIDAD COLEGIO MAYOR DE NUESTRA SEÑORA DEL ROSARIOFACULTAD DE RELACIONES INTERNACIONALES
BOGOTÁ D.C
2015

“Incidencia de las agresiones a la seguridad cibernética en el desarrollo informático de las Fuerzas Armadas de Estados Unidos (2003-2013)”

Monografía de Grado

Presentado para optar por el título de Internacionalista

En la Facultad de Relaciones Internacionales

Universidad Colegio Mayor de Nuestra Señora del Rosario

Presentado por:
Nicole Vanessa Torres Vargas

Dirigida por:
Juan Nicolás Garzón Acosta

Semestre I, 2015

RESUMEN

La presente investigación tiene como objetivo analizar la incidencia de las agresiones cibernéticas en el desarrollo informático de las Fuerzas Armadas de Estados Unidos. Los diferentes estudios que se han realizado sobre el ciberespacio se han enfocado en el papel del individuo como actor principal y se ha dejado de lado las repercusiones que éste ha tenido para el Estado, como un nuevo eje de amenazas. Teniendo en cuenta lo anterior, esta investigación demostrará a partir del concepto de securitización, que se busca priorizar la "ciberseguridad" dentro de la agenda del gobierno estadounidense. Al ser este un estudio que aborda experiencias concretas durante un periodo de tiempo de más de 10 años, el diseño metodológico de la investigación será longitudinal, ya que abarcará estudios, artículos, textos y resoluciones que se han realizado desde 2003 hasta la actualidad.

Palabras clave: *seguridad cibernética, securitización, tecnología informática, U.S CYBERCOM*

ABSTRACT

This research aims to analyze the impact of cyber-attacks in the computer development of the Armed Forces of the United States. The various studies that have been developed on cyberspace have focused primarily on the individual's role as a major player and have largely ignored the impact that this has had on the State, as a new axis of threats. Given the above, this research based on the concept of securitization, will show that since 2003, U.S. governments have prioritized "cyber security" within their political agenda. Since this is a study that addresses specific experiences over a period of more than 10 years, the methodological design of the research is longitudinal, and will cover studies, articles, texts and resolutions that have been made since 2003 to the present.

Key words: *cyber security, securitization, information technology, U.S CYBERCOM*

CONTENIDO

INTRODUCCIÓN 7

1. LA AMENAZA DEL SIGLO XXI 9

1.1 Inicios de la tecnología informática 9

1.2 El virus informático: un nuevo tipo de arma 11

1.3 La fragilidad de Estados Unidos en el ámbito cibernético 12

1.4 China: Principal amenaza de Estados Unidos en el ciberespacio 18

2. DESARROLLO CIBERNÉTICO DE ESTADOS UNIDOS 22

2.1 Las primeras acciones oficiales frente a una nueva amenaza 22

2.2 Creación de instituciones direccionadas al manejo del ciberespacio 26

2.3 Creación de un marco legal para el ciberespacio 32

3. IMPLEMENTACIÓN DE LA TEORÍA DE SECURITIZACIÓN AL CASO DE ESTADOS UNIDOS 37

3.1 Qué es “Estado” y “seguridad”? 37

3.2 Cómo surgen las amenazas? 42

3.3 La securitización del ciberespacio por parte de Estados Unidos 46

4. CONCLUSIONES 54

5. BIBLIOGRAFÍA 57

LISTA DE TABLAS Y GRÁFICOS

Cuadro 1.

Escala de sistema de seguridad instaurado para determinar nivel de peligro frente a una amenaza 15

Cuadro 2.

Componentes de la infraestructura crítica y la agencia gubernamental encargada 23

Gráfico 1. Documentos gubernamentales sobre las capacidades defensivas y de accionar de Estados Unidos en el ámbito cibernético 25

Gráfico 2. Organismos gubernamentales creados para supervisar e implementar el accionar estadounidense en el ciberespacio 30

LISTA DE SIGLAS

DARPA	Defense Advanced Research Projects Agency
DOD	Department of Defense
DHS	Department of Homeland Security
EPL	Ejército Popular de Liberación (China)
JFCC-NW	The Joint Functional Component Command – Network Warfare
JTF-GNO	Joint Task Force-Global Network Operations
NMS-CO	The National Military Strategy for Cyberspace Operations
NSA	National Security Agency
OEA	Organización de Estados Americanos
STRATCOM	United States Strategic Command
USCYBERCOM	United States Cyber Command

INTRODUCCIÓN

La tecnología se ha convertido en parte fundamental de las sociedades contemporáneas, por lo que cada vez y con mayor rapidez, se dan grandes saltos en el desarrollo de bienes y servicios tecnológicos. Se puede decir que el desarrollo informático tiene sus bases en asuntos militares y su transformación se dio en un espacio temporal relativamente corto. A partir de la década de los 90 la informática se convirtió en un asunto público y la acogida del internet y los computadores en nuestra sociedad, marcaron el inicio de la era digital. Así mismo, el Estado ha incorporado estas tecnologías con el fin de proporcionar su seguridad frente a nuevas amenazas. La tecnología informática, y por consiguiente el ciberespacio, se han convertido en un componente importante para la sociedad y el Estado de igual manera.

Sin embargo, el ciberespacio también ha dado lugar a nuevos tipos de amenaza que van desde lo leve (robo de identidad) a lo apremiante (ataque a red eléctrica, control sobre sistema de defensa). Para contrarrestar esta amenaza que surgió en los últimos años, Estados Unidos tomó ciertas medidas con el fin de incrementar su capacidad de proporcionar la seguridad en el ciberespacio.

La presente monografía busca mostrar la relación que existe entre el desarrollo informático de las Fuerzas Armadas de Estados Unidos y los ataques cibernéticos en su contra con el fin de aplicar el concepto de securitización de Barry Buzan. De acuerdo con lo anterior, se plantean como propósitos fundamentales: Describir las agresiones cibernéticas a Estados Unidos a partir del 2000 hasta 2013, identificar avances en el desarrollo informático de Estados Unidos a partir del 2003 hasta 2013, describir y analizar los diferentes elementos teóricos de la securitización.

Igualmente, el presente trabajo busca dar respuesta a la siguiente pregunta: ¿Cuál es la incidencia de las agresiones a la seguridad cibernética en el desarrollo informático de las Fuerzas Armadas de Estados Unidos desde el 2003? De esta manera, la hipótesis que se plantea para responder a esta pregunta es que las agresiones cibernéticas incidieron en el desarrollo informático de las Fuerzas Armadas de Estados Unidos, en la medida en que hicieron públicas las falencias de la seguridad cibernética estadounidense. Como respuesta

a esta problemática, el gobierno (George W. Bush y Barack Obama) llevó a cabo un proceso de securitización que tuvo como resultado la institucionalización del fenómeno cibernético dentro de los órganos de defensa y seguridad de Estados Unidos.

Para entender por qué y cómo Estados Unidos ha priorizado el ciberespacio como una amenaza a su seguridad nacional, es necesario recurrir a la teoría de securitización de Barry Buzan. Siendo así, resulta prioritario entender y explicar conceptos como Estado y seguridad, ya que constituyen la base de la seguridad nacional. Esto con la finalidad de ser usados para implementar la securitización de Barry Buzan al caso de Estados Unidos.

1. LA AMENAZA DEL SIGLO XXI

1.1 Inicios de la tecnología informática

La tecnología ha acompañado a la humanidad desde sus inicios y ha hecho posible la era de la modernización. Podemos ver que el desarrollo de la humanidad es paralelo al desarrollo de tecnologías. Fuego, armas de hierro, pólvora, y tecnología nuclear son unos de los avances tecnológicos más importantes y que más han transformado la humanidad. A esta lista se puede sumar la tecnología informática, una invención relativamente reciente, que ha tenido efectos profundos en la sociedad.

Curiosamente, la tecnología informática debe su creación en gran parte a los Estados y en especial, a la guerra. El siglo XX fue testigo de una explosión de invenciones que revolucionaron la forma en que vivían las personas (televisores, microondas, etc.). Sin embargo, fueron las guerras (Primer Guerra Mundial, Segunda Guerra Mundial, y Guerra Fría) las que impulsaron la innovación tecnológica que daría lugar a la era digital. A esto se suman instituciones como Massachusetts Institute of Technology (MIT) y Stanford University, y compañías como IBM y Hewlett Packard que hicieron posible la creación de computadores y redes. (ComputerHistoryMuseum, 2012)

El primer computador fue creado en Estados Unidos bajo el nombre de Atanasoff-Berry, a comienzos de 1940 en los laboratorios de la Universidad de Iowa. (ComputerHistoryMuseum, 2012) Según Atanasoff, este fue el primer computador digital (sus predecesores eran análogos) lo cual marcó un avance tanto en la estructura del computador como en sus funciones, los computadores pasaron de ser "calculadoras eficientes a maquinas con capacidad de memoria" (ComputerHistoryMuseum, 2012). Por su parte, Konrad Zuse, creó numerosas computadoras como "el z1, z2 y z3 bajo financiación del régimen nazi que tenían como finalidad el desarrollo de radares de mayor precisión" (ComputerHistoryMuseum, 2012).

Los inventos mencionados son un preludio a lo que fue el gran transformador de la era informática. El ENIAC, desarrollado en la Universidad de Pensilvania, es conocido por

haber sido “la primera máquina que utilizó más de 2.000 tubos de vacío (18.000 tubos de vacío)” (ComputerHistoryMuseum, 2012), convirtiéndose en la computadora más eficiente de su tiempo y a su creador, IBM, en líder indiscutible de la innovación computacional.

Para la década de los 70’s se dio una explosión de computadores personales y se abrió el mercado informático al público. La competencia entre IBM y Apple daría lugar en las siguientes décadas al rápido desarrollo del mercado informático, el cual, cada vez tomaba más popularidad en sectores financieros y gubernamentales.

Sin embargo, el desarrollo del computador no era suficiente para instaurar la era digital. Las redes que conectaban dichos computadores en todo el mundo son esenciales para el efecto transformacional de la informática. A finales de 1966, Lawrence Roberts y DARPA (DefenseAdvancedResearchProjects Agency) desarrollaron el concepto de redes informáticas, de este proyecto se desarrolló ARPANET, el precursor de INTERNET. Para 1969, el trabajo de numerosas universidades (la Universidad de California y UCLA, SRI Internacional, y la Universidad de Utah), el departamento de defensa de EE.UU, e investigadores como Roberts dio lugar al primer mensaje enviado de una universidad a otra. En octubre de 1972, DARPA organizó una gran demostración de ARPANET, en la Conferencia Internacional de Comunicaciones por Computadora (ICCC), esta fue la primera demostración pública de esta nueva tecnología de red para el público.

En 1983, como resultado del éxito del ARPANET, se decidió dividir este proyecto para que militares y universidades desarrollarán diferentes objetivos. De esta manera, ARPANET sería de uso civil mientras que MILNET sería de uso exclusivo de militares. (Internet Society, 2014) Esta década fue definitiva puesto que en 1988 Bill Morris difundió el primer virus informático y en 1990 se creó theWorld Wide Web (la versión de internet que se popularizara en los siguientes años alrededor del mundo).

1.2 El virus informático: un nuevo tipo de arma

En 1983, Fred Cohen de la Universidad del Sur de California definió el concepto de un *virus informático* como cualquier programa que pudiera modificar otros programas y, posiblemente, auto-replicarse. Técnicas de defensa ante virus informáticos fueron iniciadas por su investigación y otros expertos en informática. Según otro conocedor del tema, John Von Neumann, al fomentar la auto-copia y la capacidad de transmitir su programación a su progenie, las maquinas adquieren esta característica (se pueden conocer como virus y no como un programa informático normal). El primer programa informático catalogado como virus se dio a conocer en 1972, creado por Robert Thomas Morris "para atacar a las máquinas IBM Serie 360 de 1972, y emitía periódicamente en la pantalla el mensaje: I'm a creeper… catch me ifyou can!" (Escuela Universitaria de Informática, Madrid).

El virus informático se crea por medio de una serie de fórmulas matemáticas que se convierten en el lenguaje que da vida a este singular elemento dentro del mundo de la tecnología informática. Hace décadas, usar este lenguaje informático era cosa de expertos. En la actualidad, personas con poca experiencia en ingeniería de sistemas pueden programar un virus informático desde cualquier computador, convirtiéndolo así en un arma potencial.

Ya constituido el código base, se procede su introducción a la red u ordenador deseado. Existen dos tipos de virus informático para llevar a cabo ataques a un ordenador: virus de inicio (boot virus) y gusanos (troyans).El primero siendo el directo, por medio de USB o CD. De forma indirecta o por medio de gusanos, existen numerosos métodos dado el alto grado de interconectividad que ofrece el ciberespacio.(Stewart, 2014) Un gusano electrónico viaja como un archivo adjunto a mensajes, y se replica automáticamente por correo a decenas de usuarios (contactos) del correo electrónico de la víctima. Tambiénse inserta a un ordenador escondido en software, presumiendo ser un juego o cualquier otro tipo de programa para engañar al usuario; generalmente esto es solo una fachada para un virus que, al ejecutar el programa, se activa.(Universidad Autónoma de Yucatán, 2013)Similar a la forma en que un virus biológico se debe juntar con una célula, un virus

informático se debe juntar a algún otro programa o documento con el fin de activarse en determinado tiempo.

Aunque los dos anteriormente mencionados son los más comunes existen subdivisiones teniendo en cuenta en qué parte del hardware se instala u oculta el virus. Adicionalmente los virus se pueden dividir teniendo en cuenta el tiempo que demora en activarse y su longevidad.(Universidad Autónoma de Yucatán, 2013)

El virus informático se puede catalogar teniendo en cuenta su finalidad además de las características anteriormente mencionadas. Su finalidad puede ser: obtener la información que ya existe en el ordenador, espiar futuras acciones mientras el virus se esconde en el ordenador, manipular y controlar otros mecanismos o sistemas que dependen del ordenador (redes de electricidad, misiles, entre otros), o simplemente destruir el ordenador y aquellos que estén conectados a éste por medio de redes. (Escuela Universitaria de Informática, 2012) Teniendo en cuenta las numerosas posibilidades que ofrece el virus informático para hacer daño, se puede inferir que su uso puede dar ventajas económicas y militares a quien lo sepa explotar.

1.3 La fragilidad de Estados Unidos en el ámbito cibernético

En el caso particular de Estados Unidos, los ataques informáticos en su territorio son muy notorios. A partir del 2000, se puede observar un alza progresiva de transgresiones a los ordenadores de ciudadanos comunes. Según estadísticas oficiales, existe una diversidad de actividades criminales en el ciberespacio que afectan cada vez más al ciudadano estadounidense común:

> Según el reporte anual de crímenes cibernéticos de Estados Unidos, este tipo de crimen ha tenido un alza progresiva desde el 2001. Las principales fuentes de este tipo de crimen son el fraude económico, el robo de identidad, y el no pago-entrega de productos. El número de afectados en 2001 fue alrededor de 50000, hacia el 2005 el número de afectados ascendió a alrededor de 230,000. Para el año 2001, las pérdidas económicas como resultado de crímenes cibernéticos fueron de 17 millones de dólares. Esta cifra pasó a 183 millones de dólares para el 2005 teniendo en cuenta que se da un promedio de $424 en pérdida

económica por cada crimen reportado al FBI o la página del NationalCybercrimeComplaint Center (IC3, 2011).

A pesar de la gravedad de estos crímenes dentro del territorio estadounidense, estos ataques no son el único tipo de amenaza que surge del ciberespacio, pero si la que más afecta a la ciudadanía. Esta amenaza se traduce igualmente al sector público, ya que las páginas gubernamentales son el objetivo de un gran número de criminales cibernéticos. Según el Washington Post, oficiales del gobierno declararon que:

> El número de intentos de intrusión de todas las fuentes identificadas por el Pentágono el año pasado ascendieron a unos 79.000, según los funcionarios de defensa, frente a alrededor de 54.000 en 2003. De ellos, los intrusos lograron acceder a algún ordenador del Departamento de Defensa en unos 1.300 casos (Washington Post, 2005).

El caso que más ejemplifica la problemática cibernética es *Titan Rain*, denominado así por investigadores del gobierno federal de Estados Unidos. ShawnCarpenter, empleado de Sandia NationalLaboratories y el ejército estadounidense, "identificó infiltraciones a redes y páginas del gobierno el 1 de noviembre de 2003" (Time Magazine, 2005). Los intrusos aprovecharon los ordenadores de la red militar con menos seguridad para acceder a sus documentos de disco duro. Rápidamente se infiltraron, extrajeron información, y dejaron un "faro" (agujero en sistema de seguridad) para futuras transgresiones. (Time Magazine, 2005) Tiempo después Carpenter dio a conocer que esta operación era llevaba a cabo desde Corea del Sur, Hong Kong o Taiwán, antes de enviar la información a China continental. (Time Magazine, 2005) Se localizó la fuente principal de los ataques en la provincia de Guandong, China, además, Carpenter encontró que "los ataques procedían de sólo tres routers chinos que actuaban como el primer punto de conexión de una red local a Internet" (Time Magazine, 2005).

Para el 2005, era de conocimiento público que estas infiltraciones repetitivas habían atacado las redes del ejército de Estados Unidos. De igual manera se dio a conocer que empresas contratistas del Estado también habían sido objetivos de los hackers. Como se dio a conocer en TIME MAGAZINE:

> Time obtuvo documentos que muestran que desde 2003, los hackers, deseosos de acceder a los conocimientos técnicos de América, han puesto en peligro las redes seguras, que van desde la base militar de Redstone Arsenal a la NASA, hasta el Banco Mundial. En un caso, los hackers robaron el software de vuelo y planificación del Ejército. Hasta el momento, los archivos que han aspirado no están clasificados secretos, pero muchos son

> sensibles y están sujetos a las estrictas leyes de control de exportación, lo que significa que son estratégicamente tan importante como para requerir licencias del gobierno EE.UU. para uso en el extranjero (Time Magazine, 2005).

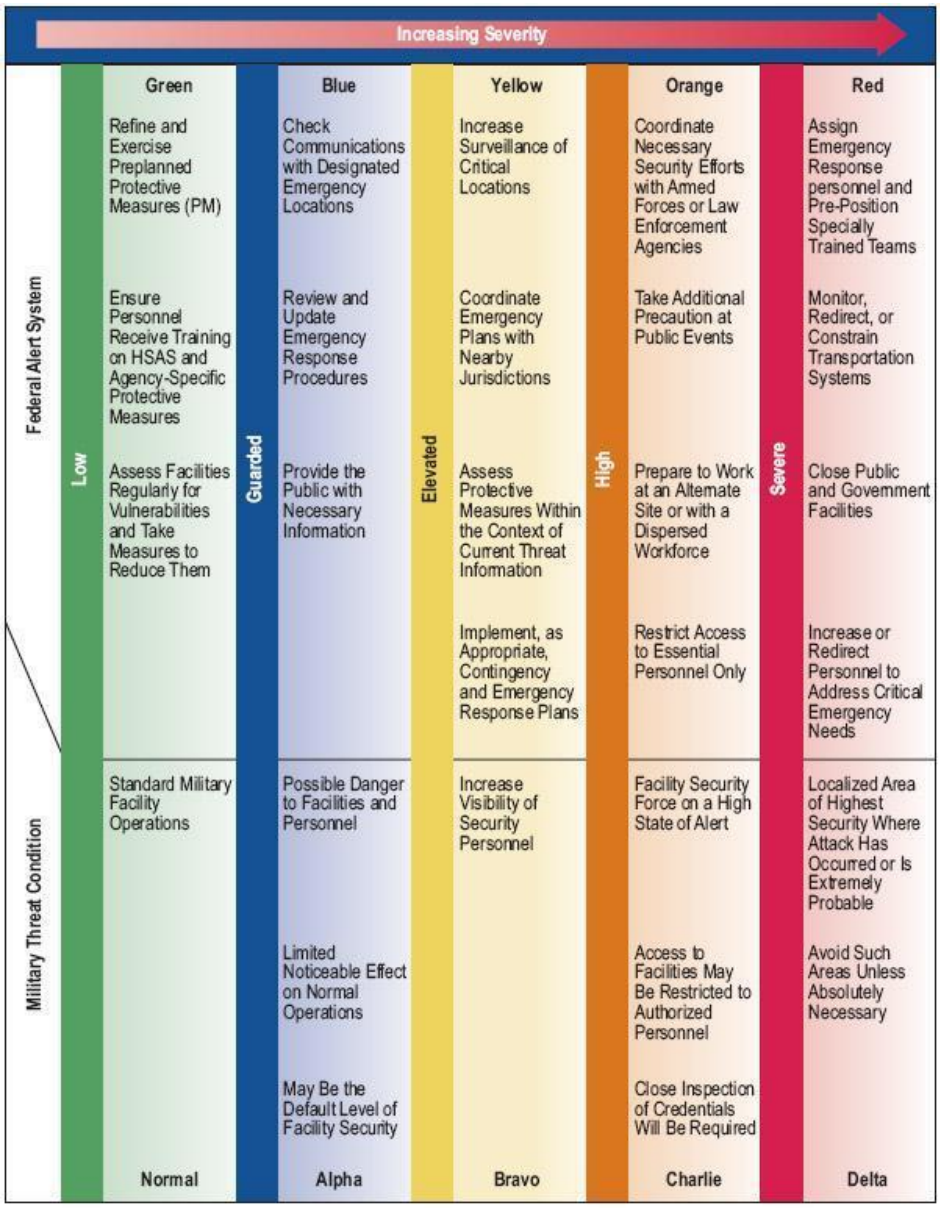
En un reporte del Congreso (CongressionalResearchServiceReportforCongress), el gobierno estadounidense por primera vez hizo mención a los ataques a sus redes. Este reporte revela los objetivos de "Titan Rain":

> Una serie de ataques informáticos lanzados en 2003 contra los sistemas del Departamento de Defensa y los sistemas informáticos pertenecientes a contratistas del Departamento de Defensa al parecer no fue detectado por muchos meses. Esta serie de ataques cibernéticos se etiquetó "Titan Rain", y se sospecha por los investigadores del Departamento de Defensa que se originan en China. Los ataques fueron dirigidos contra la Agencia de Defensa de Sistemas de Información de EE.UU. (DISA), Redstone Arsenal, las instalaciones de la Defensa Estratégica y del espacio del Ejército de Estados Unidos, y varios sistemas de cómputo críticos para la logística militar. Aunque no se violaron sistemas de información clasificada, muchos archivos fueron copiados que contienen información sensible y sujeto a las leyes de control de exportación (CRS ReportforCongress, 2007).

En el 2006, también se dio a conocer que las actividades de los hackers aún continuaban dentro del territorio estadounidense. Esta vez la red de la Naval WarCollege fue la afectada. Cabe mencionar que esta entidad se encarga de entrenar oficiales de alto rango, desarrolla y efectúa juegos de guerra y, aún más importante, lleva a cabo investigaciones clasificadas y estudios de futuros escenarios de guerra. (Washington Times, 2006)

Según Doug Gabos, portavoz de la Naval WarCollege, estos ataques estarían relacionados con el programa de investigación de la guerra cibernética que desarrolla esta entidad desde el 2002. (Washington Times, 2006)Gabos también mencionó que el ataque fue llevado a cabo el 15 de Noviembre del 2006 y dos días después el Comando Estratégico de Estados Unidos decidió elevar el nivel de alerta de seguridad de 12.000 redes informáticas del Pentágono y 5 millones de computadoras. (Washington Times, 2006)

Cuadro 1. Escala de sistema de seguridad instaurado para determinar nivel de peligro frente a una amenaza



Fuente: (Department of Transportation 2013).

El CongressionalResearchServiceReportforCongress también hace mención de estos ataques:

> En noviembre de 2006, un ataque informático prolongado contra los EE.UU. Naval WarCollege en Newport, Rhode Island, hizo que las autoridades desconectaran todas las redes de internet del campus de los funcionarios del Departamento de Defensa Internet. El Departamento de Defensa reconoce que la Red de Información Global, que es la red

> principal de los militares de EE.UU., tiene más de tres millones de escaneos diarios de posibles intrusos desconocidos (Library of Congress. 2006).

Este progresivo programa de infiltración y sustracción de información se convirtió en el primer y más conocido ejemplo de ataques informáticos dirigidos hacia Estados Unidos. Titan Rain fue el primero en su naturaleza puesto que nunca se había logrado sustraer información directamente de entes Estatales y contratistas sin ser detectado por más de tres años. También se considera como el primer ataque dirigido a Estado Unidos dentro este nuevo fenómeno cibernético denominado *cyberwarfare*(guerra cibernética). Este, sin duda, prendió las alarmas de los entes de seguridad estadounidense ya que no fue un ataque relámpago, fue un ataque reiterativo y prolongado por 3 años.

Según Alan Paller, director del SANS Institute, los problemas de Estados Unidos frente a las amenazas del ciberespacio son varios. El principal problema radica en la dependencia que tiene con respecto al internet, que según él, es más alta que sus adversarios. (UnitedStatesSenate, 2002) Incluso dice que algunos adversarios tienen la capacidad de desconectar sus sistemas y todavía tener completa funcionalidad, algo que Estados Unidos no puede hacer al 100% por su alto grado de sistematización (redes de ciudadanos, redes de comunicación, infraestructura crítica). (UnitedStatesSenate, 2002)

Pero el punto más delicado de esta situación es el mismo poderío militar del país; como máxima potencia militar del mundo, Estados Unidos cuenta con numerosos tipos de armamento que van desde bombas nucleares hasta aviones, y misiles que le dan ventaja frente a sus adversarios en cualquier campo de batalla tradicional. Pero esta ventaja desaparece cuando no se tiene mando y control sobre los equipos, lo cual puede pasar en un escenario en el cual se caigan las redes de comunicación y control de las Fuerzas Armadas. (UnitedStatesSenate, 2002)

El testimonio de Paller también detalla otro componente de esta amenaza que preocupa al gobierno. Según el director del SANS Institute, el robo de capital intelectual es igualmente problemático en el ámbito político, económico y militar. Según el informe, la "producción intelectual, fuente importante de la riqueza de Estados Unidos, se ve comprometida ante el ciberespionaje" (UnitedStatesSenate, 2002).

Como bien se sabe, Estados Unidos es una potencia industrial que debe su riqueza comercial a los grandes inventos que ha tenido a lo largo de la historia. Esto aún sigue en efecto en la actualidad, dado que Estados Unidos es un líder mundial en avances tecnólogos, médicos y militares. Hay que precisar que el robo de propiedad intelectual no es un fenómeno nuevo pero las condiciones de nuestra sociedad hacen que sus efectos sean más rápidos y más profundos. El ciberespacio se ha convertido en un medio más accesible y eficaz para sustraer propiedad intelectual, algo que antes se demoraba años ahora se puede hacer incluso antes de que se exponga al mundo las nuevas ideas. De igual manera, en la actualidad impera un mercado económico mucho más acelerado, y gracias a las líneas de producción, se puede crear productos en meses y no años. (IP ComissionReport, 2013)

Argumenta La Comisión Americana sobre Robo de la Propiedad Intelectual que este fenómeno reduce la producción e innovación de compañías americanas y de otros países desarrollados porque aquellos que adquieren la información de manera ilegal se convierten en competidores directos de los innovadores. Además, estos competidores no tienen que lidiar con los gastos de "desarrollo e innovación y talento humano, lo cual les permite reducir sus precios" (IP ComissionReport, 2013). Este círculo vicioso afecta directamente a las compañías norteamericanas, que se ven en la obligación de reducir empleados y la capacidad de innovación porque simplemente no es rentable. Ejemplo de este fenómeno lo da el mismo Alan Paller que detalla que "la base industrial de la defensa es el objetivo más valioso y fértil para las naciones que quieren robar datos de la tecnología en lugar de financiar su propia investigación de la tecnología" (U.S. SenateCommitteeonHomeland Security and GovernmentalAffairs, 2010).

Según el Almirante Haney, Comandante del Comando Estratégico de Estados Unidos, se vive actualmente un entorno de seguridad complejo, "dinámico e incierto" (SenateCommitteeOnArmedServices, 2013). En su testimonio ante el congreso, Haney añade que los avances militares de aire, tierra, y "dominios- como el espacio y ciberespacio" (SenateCommitteeOnArmedServices, 2013) han complejizado la capacidad de Estados Unidos para mantener su ventaja comparativa frente a otros Estados y actores no estatales. El más notable por supuesto es China, quien no solo busca una posición

estratégica en cuanto a poder nuclear, sino que en años recientes ha implantado planes a corto y largo plazo para obtener alta capacidad tecnológica en el ciberespacio.

1.4 China: Principal amenaza de Estados Unidos en el ciberespacio

Las autoridades estadounidenses tienen conocimiento de la aspiración China por aumentar su capacidad cibernética desde la década de los noventas. Según un estudio de capacidades cibernéticas del Instituto de Estudios de Tecnologías de Seguridad en la Universidad de Dartmouth, el objetivo principal de China durante esta década fue explorar los ataques cibernéticos como un medio asimétrico para combatir al adversario. (Institutefor Security TechnologyStudies At DartmouthCollege, 2004) De igual manera han desarrollado un plan nacional integrado, que consta de una doctrina de guerra cibernética, formación básica para sus funcionarios, y la intención de llevar a cabo ejercicios de guerra.

El informe de la Universidad de Dartmouth se apoya igualmente en las declaraciones de Michael Pillsbury, un investigador de la Universidad Nacional de Defensa de Estados Unidos, el cual dijo en 1997 que "A juzgar por sus escritos militares, están diciendo que la guerra de información es el núcleo de lo que quieren hacer", "De esta manera pueden saltar por encima de la obsolescencia de sus tanques, barcos y aviones y centrarse en la vulnerabilidad de las fuerzas de alta tecnología" (InstituteFor Security TechnologyStudies At DartmouthCollege, 2004).

Esta doctrina se puede verificar en las declaraciones que hicieron el Coronel Wang Baocun and Li Fei, para el LiberationArmyDaily. En este, Wang Baocun afirma que la estrategia de la guerra cibernética refuerza la noción de SunTzu de "someter al enemigo sin batalla" (Federation of American Scientists, 2014). Adicionalmente, dice que el objetivo de la guerra cibernética es "obligar al bando enemigo a considerar su objetivo como nuestra meta", para "forzar al oponente a renunciar a la voluntad de resistir y poner fin a la confrontación y dejar de luchar atacando la percepción y opinión de un enemigo a través de la energía de la información" (Dartmouth, 2004).

Por otra parte, el Coronel Wang afirma que existen cinco finalidades para el uso del ciberespacio: Primero, la destrucción de fondo, el uso de armas difíciles para destruir la capacidad de mando del enemigo, sus puestos de mando y control de centros de información. (Federation of American Scientists, 2014) Segundo, la guerra electrónica, el uso de medios electrónicos de interferencia o el uso de armas anti radiación (electromagnética) para atacar a los sistemas de información del enemigo y de recolección de inteligencia, como las comunicaciones y radares. Tercero, el engaño militar, el uso de operaciones como trampas tácticas [ataques simulados] para blindar o engañar a los sistemas de recolección de inteligencia enemiga. Cuarto, promover secreto operacional, el uso de todos los medios para mantener el secreto y evitar que el enemigo recolecte información de inteligencia sobre las operaciones. Por último, es la guerra psicológica, el uso de la televisión, la radio y folletos para minar la moral militar del enemigo. (Federation of American Scientists, 2014)

Varios investigadores de la Academia China de Ciencias Militares, Universidad de Defensa Nacional de China, y de la Academia de Comunicaciones del Comando Wuhan han publicado libros sobre el uso del ciberespacio en la guerra. De esta investigación, el instituto de Dartmouth concluyó que existe una gran diferencia en la visión que se tiene de los usos del ciberespacio; EE.UU. tiende a centrarse en los aspectos de ataque de la guerra cibernética, mientras que la guerra cibernética de China se centra más en operaciones psicológicas y la manipulación y engaño por medio de información. (Dartmouth, 2004) En otras palabras, la doctrina de la guerra cibernética china se centra en derrotar al enemigo antes de entrar en batalla.

Al igual que el desarrollo de su doctrina y lineamientos, la República Popular de China se ha esforzado por capacitar a sus empleados para poder llevar a cabo estas operaciones cibernéticas. Entre los centros de capacitación para la ciberguerra del EPL están la Academia de Comunicaciones Comando en Wuhan, la Universidad de Ingeniería de Información en Zhengzhou, la Universidad de Ciencia e Ingeniería y la Universidad de Defensa Nacional de Ciencia y Tecnología en Changsha. (Mandiant, 2013)

Allí se enseña a jóvenes numerosos conocimientos que incluyen: Conceptos básicos y aplicaciones informáticas, tecnología de red de comunicaciones, normas y reglamentos de guerra cibernética; estrategia de la guerra cibernética y la táctica;ciber estratégica de guerra, incluyendo la recolección, manejo , difusión y uso de la información y comandos de combate, control y toma de decisiones. (Dartmouth, 2004) Igualmente, en estas instalaciones es frecuente el uso de guerra cibernética simulada en la cual se usan virus reales para determinar la mejor forma de accionar.

Teniendo en cuenta la enorme preferencia que se le ha dado a este tema en los últimos años, es importante analizar cuánto dinero del presupuesto chino ha ido hacia el desarrollo cibernético. Para el 2003, autoridades estadounidense estimaban el presupuesto militar de China en aproximadamente 65 mil millones de dólares, de este presupuesto el gobierno chino aprobó un aumento del 9.6% para desarrollar capacidades informáticas. (CNN, 2003)

Para el 2013, se conoció el reporte de Mandiant, de la compañía que se dedica a la seguridad cibernética y en el cual se expresa gran preocupación por las reiteradas operaciones militares cibernéticas que ha llevado a cabo China desde el 2006. Esto, según Mandiant, gracias a un grupo dedicado exclusivamente a ataques y operaciones cibernéticas con sede en Gaoqiaozhen, Shanghái, China. Este grupo es conocido como la UNIDAD 61398 y está bajo el comando del tercer departamento del Departamento de Estado Mayor que, a su vez, se reporta directamente a la Comisión Militar Central del Partido Popular de China. (MandiantReport, 2013)

La evidencia que recolectó Mandiant acerca de la unidad 61398 revela una red organizada que tiene objetivos mayoritariamente en Estados Unidos (115 víctimas) como en otros países occidentales. Se concluye en este reporte que esta organización: emplea a cientos ya que requiere personal capacitado en informática y de operaciones de la red, tiene grandes infraestructuras e instalaciones en Shanghai, y fue el beneficiario de infraestructura de comunicaciones de fibra óptica especialmente proporcionada por la empresa de propiedad estatal de China Telecom en nombre de la defensa nacional. (MandiantReport, 2013)

Se conoce, además, que este grupo o unidad está operando desde 2006 y ha atacado a más de 141 organizaciones a nivel mundial. Igualmente se ha dado a conocer que estas acciones tuvieron como propósito acceder a información como propiedad intelectual, planos de tecnología, procesos de fabricación patentados, resultados de pruebas, planes de negocio y documentos de fijación de precios. (MandiantReport, 2013)

Es posible ver a partir de lo anterior que el ciberespacio se ha desarrollado hasta el punto en el cual las sociedades dependen de su dominio. Estados Unidos es uno de los más afectados por la necesidad de controlar sus redes e infraestructura crítica. Esto ha hecho que otros Estados y actores busquen un desarrollo informático para poder tener ventaja frente a un Estado que tiene una ventaja militar indiscutible. En otras palabras, estos actores buscan desestabilizar la hegemonía militar de Estados Unidos por un medio diferente a los tradicionales (tierra, aire, mar).

2. DESARROLLO CIBERNÉTICO DE ESTADOS UNIDOS

2.1 Primeras acciones oficiales frente a una nueva amenaza

Como fue descrito anteriormente, existe un enorme riesgo para la seguridad ciberespacial estadounidense. Como reacción frente a esta nueva amenaza, las administraciones de George W. Bush (2001-2009) y Barack Obama (2009- presente) tomaron ciertas medidas. Esto abarca la creación de nuevas agencias o entes de seguridad, divulgación de nuevos planes y/o estrategias, y promulgación de nuevas leyes de regulación.

Los esfuerzos por adelantar una securitización de la agenda cibernética se iniciaron en la década de los noventa. El *Report of thePresident'sCommissiononCriticalInfrastructureProtection*de 1997 mostró la preocupación de la administración Clinton por el peligro que puede significar el uso indebido del ciberespacio por parte de enemigos de Estados Unidos. Según esta investigación, se estableció que ciertos enemigos podrían adquirir la "capacidad generalizada para explotar vulnerabilidades de la infraestructura crítica de Estados Unidos a través de redes de información" (President'sCommissiononcriticalinfrastructureprotection, 1997). Para poder reflejar la gravedad del asunto, es pertinente enfatizar que la infraestructura crítica, definida por Homeland Security es:

> La columna vertebral de la economía, la seguridad y la salud de nuestra nación. Nosotros lo conocemos como el poder que usamos en nuestros hogares, el agua que bebemos, el transporte que nos mueve, y los sistemas de comunicación de los que dependemos para mantenerse en contacto con amigos y familiares. Las infraestructuras críticas son los activos, sistemas y redes, ya sea físico o virtual, tan vital para los Estados Unidos que su incapacitación o destrucción tendría un efecto debilitador sobre la seguridad, la seguridad económica nacional, la salud pública o la seguridad nacional, o cualquier combinación de los mismos (Department of Homeland Security, 2014).

El *Report of thePresident'sCommissiononCriticalInfrastructureProtection*fue la base para que la administración Clinton estableciese la directiva presidencial #63, en la cual se delimitan los pasos a seguir:

> A más tardar el año 2000, EE.UU. debe alcanzar una capacidad operativa inicial y, a no más tarde de cinco años a partir de hoy, se debe haber logrado la capacidad de proteger las infraestructuras vitales de la nación de actos intencionales (PresidentialDecisionDirective/nsc-63, 1998).

Cuadro 2. Componentes de la infraestructura crítica y la agencia gubernamental encargada

Infraestructura crítica	Agencia Gubernamental
Información y Comunicaciones	Departamento de Comercio
Banca y finanzas	Departamento de Tesorería
suministro de agua	Agencia de Protección Ambiental
Aviación, carreteras (incluyendo camiones), transporte masivo Pipelines , comercio marítimo y fluvial	Departamento de Transporte
Servicios de aplicación de la ley	Departamento de Justicia / FBI
Servicio de bomberos, continuidad de los servicios públicos	Agencia Federal para el Manejo de Emergencias
Servicios de salud pública, incluida la prevención, vigilancia, servicios de laboratorio y servicios de salud personales	Departamento de Salud y Servicios Humanos
Energía eléctrica, La producción y almacenamiento de petróleo y gas	Departamento de Energía

Cuadro elaborado por la autora del presente trabajo de grado con base en la información de (Department of Homeland Security, 2014)

En el año 2000, se dio a conocer el primer plan para la protección de los sistemas de información divulgado por la administración Clinton. El objetivo del plan era lograr la defensa de sistemas de información con una plena capacidad operativa para mayo de 2003. Cuando ese sistema de defensa estuviera en efecto, Estados Unidos debería haber alcanzado la capacidad de asegurar que: "Cualquier interrupción o manipulación de estas funciones críticas debe ser breve, infrecuente, gestionable, aislada geográficamente, y lo menos perjudicial posible para el bienestar de los Estados Unidos" (The White House, 2000).

Hasta el 2000, los intentos por hacer el ciberespacio controlable y seguro habían tenido pocos efectos reales. Por medio de la directiva presidencial y el plan nacional para la protección de los sistemas de información se buscó un objetivo general que consistía en reducir el riesgo de ataques hacia Estados Unidos. Este objetivo se centraba en la infraestructura crítica pero no existía claridad acerca de cómo se llevaría a cabo, puesto que se hace énfasis en que cada entidad asegurará sus propias redes, sin tener en cuenta que por la misma naturaleza del ciberespacio, es imposible manejar este problema de manera desagregada. Tampoco se detalló la manera en que funcionaría la llamada alianza entre entes públicos y privados para garantizar la infraestructura crítica, puesto que simplemente se enuncia sin crear lineamientos específicos. Aunque el ciberespacio ya se consideraba un campo donde se podrían materializar las amenazas, de ninguna manera constituía una de las más relevantes a comienzos del siglo XXI.

La seguridad cibernética quedó relegada a un segundo plano tras los ataques del 11 de septiembre, que precipitaron el terrorismo islámico como el objetivo principal de todas las agencias de seguridad de Estados Unidos y el mundo. Fue por esta razón que en el 2001, ahora bajo la administración de George W. Bush, se creó TheDepartment of Homeland Security (años más tarde sería pieza vital de la securitización del ciberespacio) como el ente encargado de defender la seguridad dentro del territorio estadounidense.

Aunque solo uno de sus enfoques, este departamento tenía la capacidad y responsabilidad de:

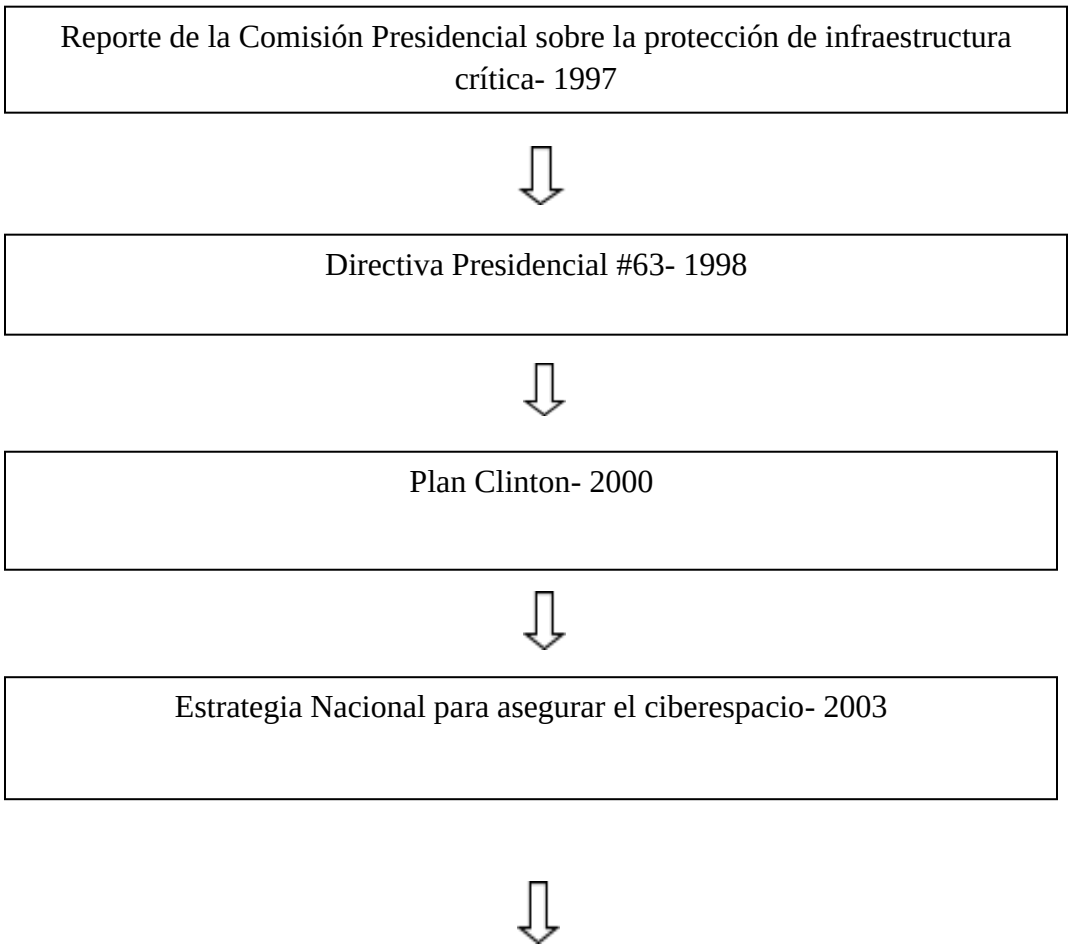
> Desarrollar un plan nacional integral para asegurar los recursos claves y críticos de la infraestructura de los Estados Unidos, proporcionar la gestión de crisis en respuesta a los ataques contra los sistemas de información críticos, y el desarrollo junto con otros organismos, de una nueva comprensión científica y tecnológica de la seguridad nacional, entre otros (Presidentialdocuments, 2001).

Para el 2001 también se estableció el Consejo Consultivo Nacional de Infraestructura (CANI), que tenía como objetivo principal proporcionar al Presidente Bush "con consejos sobre la seguridad de los sistemas de información para la infraestructura crítica de sectores de la economía: banca y finanzas, transporte, energía, manufactura y gobierno de emergencia servicios" (ExecutiveOrder 13231, 2001). También fue el primer

ente gubernamental con la función específica de mejorar la colaboración entre los sectores público y privado en la protección de sistemas de información.

Aparte del Consejo Nacional de Infraestructura y del Department of Homeland Security no existía ningún otro ente con autorización para actuar o manejar la seguridad en el ciberespacio. Dentro de los documentos oficiales publicados por Estados Unidos no se hace referencia a una intención de hacer uso militar del ciberespacio como arma o de especializar las Fuerzas Armadas para la defensa informática. Se puede decir que hasta el 2001 se tenía una visión superficial de las amenazas que podrían emerger del ciberespacio y, por lo tanto, no se tenía un objetivo claro respecto a la reacción del gobierno frente al desarrollo informático de otros países porque se enfocaba en el accionar de grupos terroristas.

Gráfico 1. Documentos gubernamentales sobre las capacidades defensivas y de accionar de Estados Unidos en el ámbito cibernético



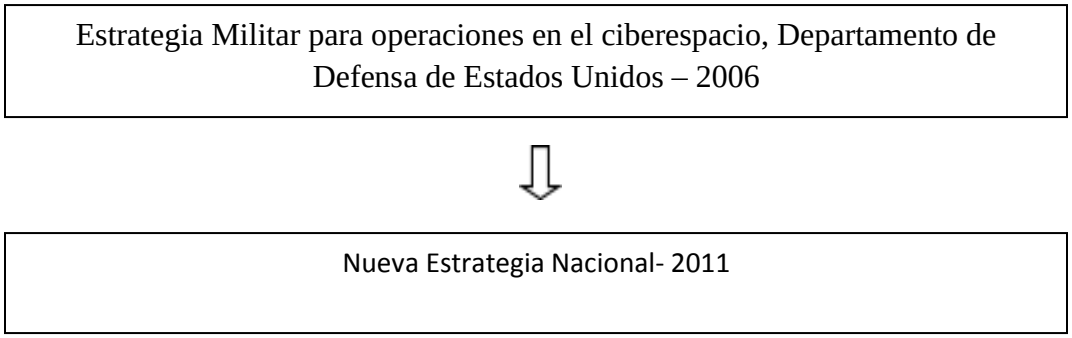


Gráfico elaborado por la autora del presente trabajo de grado con base en la información de (Department of Defense, 2011), (Department of Homeland Security, 2001), (Department of Defense, 2003), (TheWhitehouse, 1998),

2.2 Creación de instituciones direccionadas al manejo del ciberespacio

Solo es hasta el 2003 que se empieza a incluir el ciberespacio como amenaza inminente dentro de la agenda de la administración Bush. Es en este año cuando por primera vez se implementan instituciones adheridas a las Fuerzas Armadas de Estados Unidos para este objetivo específico. De esta manera, la administración Bush publicó la primera estrategia nacional para asegurar el ciberespacio en febrero del 2003. Este documento contenía cinco grandes prioridades para enfrentar la amenaza del ciberespacio. Por primera vez el gobierno hablaba de crear un sistema de respuesta nacional para el ciberespacio (anteriormente se hablaba de un plan, no de un sistema físico y concreto), dentro de este sistema se propone "ampliar la red de información y de alerta del ciberespacio para apoyar el papel del DHS en la coordinación de la gestión de crisis de la seguridad del ciberespacio" (The White House, 2003), lo cual plantea que otras agencias y departamentos se involucren en la gestión de asegurar el ciberespacio.

La segunda prioridad de esta estrategia fue crear un programa de reducción de vulnerabilidad que propone específicamente asegurar "los mecanismos de internet mediante la mejora de los protocolos y enrutamiento" y "mejorar las capacidades de aplicación de la ley para prevenir y perseguir los ataques cibernéticos" (The White House, 2003). Los

puntos anteriores muestran un grado de especificidad en el tema mayor al que se manejaba en el 2001, ya que en el primero se hace referencia a acciones técnicas y la segunda de acciones legales nuevas para enfrentar ataques.

El tercer punto trata asuntos como la innovación en el manejo de la tecnología informática dentro del gobierno puesto que reitera la importancia de la creación de un programa de formación para la seguridad nacional en el ciberespacio. (The White House, 2003) Por primera vez el gobierno habla de concientizar a la población general sobre las amenazas del ciberespacio y además de entrenar y educar a funcionarios para que puedan suplir las necesidades de la seguridad cibernética.

El cuarto punto de la estrategia nacional para el ciberespacio priorizala seguridad de las redes federales, de uso estricto del gobierno y ejército. Para esto se propone limitar el número de entes que tienen acceso a este tipo de red, asegurar el uso inalámbrico dentro de la red, y por último, incentivar a gobiernos locales para que desarrollen programas de seguridad para sus redes. (The White House, 2003)

El quinto y último punto, es tal vez el más relevante puesto que describe la intención de Estados Unidos por desarrollar la cooperación internacional para la seguridad en el ciberespacio. La voluntad expresada anteriormente demanda fortalecer la contrainteligencia, mejorar las capacidades para la atribución de ataques, mejorar la coordinación para responder a los ataques cibernéticos en la comunidad internacional, y establecer redes internacionales de vigilancia. (The White House, 2003) Por último se alienta a otros países a que se adhieran al Convenio del Consejo de Europa sobre la Ciberdelincuencia, el cual es "el primer tratado internacional que busca hacer frente a la ciberdelincuencia mediante la armonización de las leyes nacionales, la mejora de las técnicas de investigación, y el incremento de la cooperación entre las naciones" (The White House, 2003).

En adición a los esfuerzos de Department of Homeland Security, también se crearon*The Joint Functional Component Command – Network Warfare (JFCC-NW) yJoint Task Force-Global Network Operations (JTF-GNO),* ambos en 2005 (United States Strategic Command, 2014). Estos dos comandos estaban subordinados al

UnitedStatesStrategicCommand- STRATCOM, uno de los nueve comandos unificados del Departamento de defensa.(UnitedStatesStrategicCommand, 2014) La primera tenía la función primordial de coordinar operaciones ofensivas en redes informáticas mientras que la segunda se encargaba de mantener y asegurar la red de comunicación para uso estratégico del Departamento de Defensa. (The White House, Febrero 2003)

Siguiendo los planteamientos de la estrategia nacional, que consistían en que cada agencia y departamento desarrollara sus propias iniciativas para asegurar el ciberespacio, la Fuerza Aérea de Estados Unidos proclamó, el 3 de diciembre del 2006, la creación de un cibercomando. La misión de la Fuerza Aérea de los EE.UU era ofrecer opciones soberanas para la defensa y los intereses en el aire, espacio y ciberespacio. De esta manera, la Fuerza Aérea manifestó que: "El Comando Operacional Ciberespacio debe permitir el empleo de poder ciberespacial global a través de todo el espectro del conflicto, tanto como apoyo y / o componente de apoyo de una fuerza conjunta" (Thesecretary of the U.S Air Force, 2006). Sin embargo, solo fue hasta el 2009 cuando se creó la división 24 de la Fuerza Aérea, que institucionalizó las operaciones informáticas dentro de la Fuerza Aérea. Bajo esta división se estableció la 68th WING (operaciones informáticas), 67th WING (guerra informática), 689th WING (operación de contrainteligencia), y la 624th WING (encargada de coordinar operaciones informáticas). (24th Air Force Home page, 2014)

En el caso del ejército, su centro de informática tuvo sus comienzos en 1998 con la *9 división* que tenía la misión de proteger las redes informáticas de uso exclusivo del ejército. A comienzos del siglo XXI, esta división y sus propósitos fueron transformados para crear el primer comando de operaciones informáticas del ejército (1st IO COM) y NETCOM. (ArmyCyberCommandHomepage, 2014) La primera capacitada para practicar y llevar a cabo operaciones militares cibernéticas y guerra electrónica y la segunda encargada, como su antecesor, de la defensa de las redes informáticas de ejército.

La marina (U.S Navy) también dio lugar a divisiones cibernéticas dentro de su organización. En 2010, se creó la Décima Flota (10th Fleet), única encargada de criptología para uso de la Marina de Estados Unidos, además de encargarse de operaciones cibernéticas y operación de guerra electrónica. (NavyForceHomepage, 2014) En 2013, la marina declaró

que para 2017 esta división estaría dotada de equipos de defensa y ataque que mitiguen la vulnerabilidad de Estados Unidos en el dominio del ciberespacio. Igualmente, el Cuerpo de Marina (Marine Corps), otro Servicio dentro de las Fuerzas Armadas de Estados Unidos, estableció un comando cibernético para facilitar sus propias operaciones futuras.

Para el 2006, el Departamento de Defensa implementó lo que llamó "TheNationalMilitaryStrategyforCyberspaceOperations (NMS-CO)" (Departamento de Defensa, 2006). Su finalidad era ampliar el papel de este departamento en la defensa nacional e integrar las operaciones en el ciberespacio. Como bien lo dice el documento, el ciberespacio es el primer dominio estratégico creado por el hombre, los demás dominios son parte de la naturaleza que nos rodea y es en esta diferencia que radica la ambigüedad de este campo de acción. (Departamento de Defensa, 2006) El documento trata de especificar las amenazas hacia Estados Unidos pero se limita a describir tipos de amenazas sin nombrar agentes o actores específicos.

Menciona que existen amenazas tradicionales provenientes de países con capacidad tecnológica y hostilidad hacia Estados Unidos y sus intereses; amenazas irregulares o asimétricas que provienen de grupos terroristas que buscan desestabilizar Estados Unidos por medio de ataques a infraestructura y población; y amenazas catastróficas que buscan controlar y usar armas de destrucción masiva. (Departamento de Defensa, 2006) Aunque estas son las amenazas prioritarias también existen amenazas disruptivas, es decir, amenazas en las cuales un segundo actor obtiene tecnológica avanzada que disminuye la ventaja comparativa de Estados Unidos en el ciberespacio. (Departamento de Defensa, 2006)

Teniendo esto en cuenta, se decide en 2009 la reorganización de todas las instituciones existentes y la creación de nuevos entes para mejorar el intercambio de información entre los Servicios de las Fuerzas Armadas de Estados Unidos. Se eliminan así The JointFunctionalComponentCommand – Network Warfare (JFCC-NW) y JointTaskForce-Global Network Operations (JTF-GNO) para dar paso a la creación del U.S Cyber Command, el 23 de Junio del 2009.(Department of Defense, 2003) El USCYBERCOM, como sus antecesores, estaría subordinado a STRATCOM. A su vez, esta

entidad recién creada tendría bajo su mando a las 5 servicios militares que anteriormente manejaban este tema individualmente (Department of Defense, 2003). Con esto, los Servicios dentro ejército, marina, fuerza aérea y cuerpo de marines serían mucho más efectivos en su cooperación y desarrollo conjunto para asegurar el ciberespacio.

En 2011, el Departamento de Defensa publicó la continuación de la estrategia nacional para asegurar el ciberespacio de 2003. En este nuevo documento, se describen 5 estrategias a seguir por el gobierno y las agencias capacitadas para asegurar el ciberespacio. Primero el Departamento de Defensa tratará el ciberespacio como un dominio operacional para el cual se debe organizar, equipar espacios físicos y entrenar al personal de manera que pueda aprovechar al máximo el potencial del ciberespacio. (Department of Defense, 2011) Otro punto de esta estrategia muestra la dependencia que tiene el gobierno con el sector privado:

> Muchas de las funciones y operaciones críticas del Departamento de Defensa se basan en los activos comerciales, incluyendo proveedores de servicios Internet (ISP) y las cadenas de suministro mundiales, sobre los que el Departamento de Defensa no tiene autoridad directa para mitigar el riesgo con eficacia. Por lo tanto, el Departamento de Defensa colaborará con el Departamento de Seguridad Nacional (DHS), otros socios entre agencias y el sector privado para compartir ideas, desarrollar nuevas capacidades, y apoyar los esfuerzos colectivos para hacer frente a los desafíos transversales del ciberespacio (Department of Defense, 2011).

La estrategia también desarrolla un punto de cooperación internacional, en el cual se procura generar capacidades de sensibilización y alerta de situaciones compartidas que permitan la legítima defensa colectiva y la disuasión colectiva. También proponía avanzar en el desarrollo y promoción de las normas internacionales del ciberespacio y los principios que promueven la apertura, la interoperabilidad, la seguridad y la fiabilidad. Por último se buscó fomentar "la educación y formación de iniciativas, la adopción y la ampliación de los programas de tutoría intergeneracionales permitirán al Departamento de Defensa crear una base de talento cibernético dotado para las futuras misiones de defensa y seguridad nacional" (Department of Defense, 2011).

Gráfico 2. Organismos gubernamentales creados para supervisar e implementar el accionar estadounidense en el ciberespacio

Department of Homeland Security

⇩

Consejo Consultivo Nacional- 2001

⇩

The Joint Functional Component Command- 2005, The Joint Task Force Global Network Operations- 2005

⇩

Ciber comando Fuerza Aérea- 2006

- División 24 Fuerza Aerea- 2009
- 67th Wing (Guerra informática)
- 689th Wing (contrainteligencia)
- 624thWing (Coordinación de Operaciones Informáticas)

⇩

Cibercomando Ejército (U.S Army)

- 9th division- 1998
- 1st IOCOM (comando de operaciones informáticas)- 2000
- NETCOM (defensa informática)- 2000

⇩

Marina (U.S Navy)

- 10th Fleet (criptologia)- 2010
- para 2017 debe estar capacitada para operaciones informáticas de defensa y ataque

⇩

USCYBERCOM

- Se eliminan The Joint Functional Component Command y The Joint Task Force Global Network Operations para crear USCYBERCOM (comando general del ciberespacio.
- Está subordinado a STRATCOM
- Reúne a todos los cibercomandos creados por Fuerza Aérea, Ejército, Marina, y Marine Corps para facilitar el intercambio de información e incrementar las operaciones informáticas conjuntas.

Gráficoelaborado por la autora del presente trabajo de grado con base en la información de(ArmyCyberCommand, 2013), (UnitedStatesNavy, 2013), (SenateCommitteeOnArmedServices, 2014), (President'sCommissiononcriticalInfraestructure, 2012)

2.3 Creación de un marco legal para el ciberespacio

En el ámbito legal se adelantaron iniciativas que respaldaran las acciones de las agencias gubernamentales. Las primeras regulaciones estaban encaminadas a salvaguardar información privada y delicada del gobierno y los ciudadanos. Las tres principales leyes de seguridad cibernética son: la ley de Portabilidad y Responsabilidad de seguro social de 1996 (HIPAA), la Ley Gramm-Leach-Bliley de 1999, y la Ley de Seguridad Nacional de 2002, que incluyó la Ley Federal de Información de Gestión de Seguridad (FISMA). La más relevante de estas es la ley FISMA, promulgada en el año 2002 reconociendo la importancia de la seguridad de la información en los intereses económicos y de seguridad nacional de Estados Unidos. Esta ley busca crear un ambiente en el cual cada agencia federal desarrollé, documenté e implementé un programa para proporcionar seguridad a los sistemas de información. (Bureau of consumerprotection, 2014) En conjunto, estas tres leyes exigen que las organizaciones de salud, instituciones financieras y agencias federales protejan sus sistemas y la información de ataques enemigos. (Bureau of consumerprotection, 2014)

Para acompañar estas leyes, también se crearon "cybercrimelaws" o leyes para crímenes en el ciberespacio. En estas leyes, que rigen y controlan el uso del ciberespacio dentro del territorio estadounidense, se detallan crímenes habituales dentro de la sociedad

norteamericana. Delitos como fraude, vulneración de derechos de autor, falsificación de documentos, robo de identidad, distribución de material obsceno, espionaje y robo de información son algunos de los crímenes cibernéticos que se busca reducir con la introducción de estas leyes. (Organización de Estados Americanos [OEA], 2006) Estas leyes fueron compiladas en 2006 por la OEA como modelo a seguir, ya que en ese momento existían pocos Estados que incluyeran el cibercrimen en su cuerpo normativo. Esto ha impactado directamente el tipo de regulación que quiere llevar a cabo la OEA, la cual es detallada en la Declaración de las Américas para la Ciberseguridad de 2012. (OEA, 2006)

En años recientes, el legislativo norteamericano ha gestionado leyes dirigidas a la regulación del ciberespacio. Entre estas se puedenresaltartres: S. 3414 (112th): CSA2012, S. 2151 (112th), S. 2105 (112th): Cybersecurity Act of 2012. (GovTrack, 2014) Todas estas iniciativas tienen propósitos en común, ya que están encaminadas a fortalecer la seguridad cibernética de Estados Unidos y las estrategias cibernéticas divulgadas por administraciones anteriores. (Estrategia para ciberespacio 2003 y plan para la seguridad ciberespacial 2011) Para esto, las regulaciones legislativas propuestas buscan establecer programas de educación para futuros empleados de las agencias de seguridad, además de suplir las vulnerabilidades en cada paso de la relación mutuamente dependiente pública-privada y la protección de la infraestructura crítica.

Igualmente, estas iniciativas han sido acompañadas por otros dos grandes proyectos para facilitar el trabajo de las agencias de seguridad. La ley H.R. 3523, añade disposiciones relativas a la información sobre amenazas cibernética y el intercambio de información(GovTrack, 2012). Sin embargo, esta ley no tuvo éxito ya que no contó con la votación suficiente en la Cámara de Representantes.

Muchos de los detractores de esta ley resaltaban la falta de protección a la privacidad de los ciudadanos estadounidenses y el alto margen de actuación que se otorgaba a las agencias de inteligencia. Hoy se sabe que ninguna de estas leyes pasó el debate en la cámara porque existían fuertes críticas acerca de qué tanta información debe

ser suministrada al Estado para que puede proveer seguridad sin afectar los intereses de las empresas y el derecho de cada ciudadano a la privacidad. (GovTrack, 2011)

El fracaso de estas leyes se atribuye a los escándalos de wikileaks y Edward Snowden, en los cuales se dio a conocer el espionaje del gobierno a ciertas páginas (Facebook) de uso público. Así pues, la ciudadanía no ve con buenos ojos cualquier proyecto de ley que insinué respaldar el accionar gubernamental en el ciberespacio. De esta manera, sacar adelante una ley que proteja la privacidad de los cibernautas y que, igualmente, permite un alto grado de acción al gobierno es el objetivo del ejecutivo. Sin embargo, esta iniciativa no tiene gran acogida en la fracción republicana del legislativo, puesto que ven en la regulación o control del ciberespacio la limitación de su potencial económico y social.

La otra ley pertinente a este estudio, denominada HR 624 (Ley de Intercambio de Inteligencia y Protección del Ciberespacio), "Dirige el gobierno federal para llevar a cabo actividades de ciberseguridad para proporcionar conocimiento de la situación compartida que permite acciones operativas integradas para proteger, prevenir, mitigar, responder y recuperarse de incidentes cibernéticos" (GovTrack, 2013).

Se puede resumir que esta ley quiere resaltar y crear un sistema que permita el cuidado de la información de los centros de inteligencia. Se pretende limitar las agencias y el personal que tiene acceso a esa información de la cual gran parte es clasificada. También se resalta la importancia de respetar los derechos de los usuarios cibernéticos al momento de recolectar inteligencia dentro de estas agencias. Como se estipula en la Carta de Derechos de Estados Unidos (Bill of Rights), los ciudadanos estadounidenses tienen derecho a la privacidad y la libertad de expresión, entre otros, lo cual limita la capacidad del Estado para vigilar todas las interacciones que se dan en el ciberespacio. (GovTrack, 2013)

De acuerdo a lo detallado anteriormente, se pueden concluir ciertos puntos. Primero, solo es hasta los primeros años del siglo XXI que el gobierno estadounidense comienza a tomar el ciberespacio como una amenaza real y latente para su seguridad y supervivencia. Esto se puede relacionar con los numerosos ataques cibernéticos que sufrió Estados Unidos

en este mismo tiempo, entre los que se destaca las operaciones denominadas Titan Rain. Segundo, como respuesta a esta amenaza, el gobierno estadounidense impuso su intención de especializar sus Fuerzas Armadas y agencias de seguridad en el ámbito informático para poder hacer frente y reducir las vulnerabilidades del país en este nuevo dominio militar. Para esto se crearon estrategias e iniciativas que encaminaron el rumbo a seguir para alcanzar esta meta, entre las cuales se destacan, la estrategia para el ciberespacio de 2003 y la estrategia para el ciberespacio de 2011.

Siguiendo los lineamientos propuestos en las estrategias descritas, el paso a seguir fue la creación de cibercomandos dentro de las Fuerzas Armadas (ejército, marina, fuerza aérea, cuerpo de marina, guardia costera). Esto tuvo como resultado la unificación de estos cibercomandos en uno solo denominado U.S Cyber Command, el cual se institucionalizó en el 2010 para facilitar el rápido intercambio de información y la eficiente respuesta ante ataques.

Estos organismos estatales dedicados a la ciberseguridad tienen ciertos propósitos descritos entre los cuales se destacan: asegurar la defensa de las redes informáticas del gobierno y ejército, mejorar la defensa de la infraestructura crítica de Estados Unidos, incrementar la capacidad de detectar y responder ante posibles ataques cibernéticos, permitir el intercambio de información entre entes especializados en este tema, disminuir la capacidad de enemigos de llevar a cabo operaciones militares (espionaje, inteligencia, actos de guerra con repercusión física, entre otros),e incrementar la capacidad de Estados Unidos de llevar a cabo "cyberwarfare" o guerra informática.

Para poder llevar a cabo estos propósitos dentro del ámbito legal, el congreso estadounidense y el poder ejecutivo han desarrollado ciertas leyes que regulan y permiten la actuación militar en el contexto del ciberespacio. Parte de estas leyes se denominan "cybercrimelaws" y son aquellas dirigidas a atacar las faltas menores dentro del ciberespacio como el fraude y el robo de identidad, y en últimas, busca regular el manejo de los ciudadanos en el ciberespacio. También se han creado leyes que se dirigen a los entes públicos y privados (grandes compañías, gobierno, y entes de salud) que manejan grandes cantidades de información privada de ciudadanos.

De igual manera, existen leyes que se dirigen específicamente al comportamiento de las agencias de seguridad y entes militares con capacidad de accionar en el ciberespacio. Esta ley (HR 624, Ley de Intercambio de Inteligencia y Protección del Ciberespacio) otorga el derecho a llevar a cabo operaciones militares a ciertos entes militares bajo dirección de los altos mandos de DOD y DHS. Además se especifica que estas agencias no pueden quebrantar el derecho a la privacidad y libertad de los ciudadanos usuarios del ciberespacio, este es un aspecto clave debido a los recientes escándalos de espionaje a redes sociales, líneas telefónicas y páginas de correo electrónico por parte de la NSA.

Esta ley hace énfasis en el control y manejo que se debe dar a la información que tienen estas agencias, y dispone un manejo más restringido para evitar otro escándalo como el de Edward Snowden, quien divulgó información clasificada y sensible para la seguridad nacional de los Estados Unidos.

Por último, se puede concluir que Estados Unidos ha mostrado un gran esfuerzo por crear un marco legal e institucional que regule el ciberespacio, sin embargo, esto no ha tenido efecto alguno en contra de las amenazas de alto grado operacional (como lo son otros Estados y entre estos China). Esto se debe principalmente a que estas leyes disuaden los delitos cibernéticos de poca complejidad entre los mismos ciudadanos estadounidenses y que, gracias a su conocimiento operacional básico, son fáciles de descubrir. Pero esta regulación no tiene efecto alguno en hackeos y ataques internacionales que persisten y aumentaron en gravedad en la última década. Se puede ver que las regulaciones no reducen la fragilidad de la defensa cibernética estadounidense y tan solo exponen la incompetencia de este país para proporcionar su seguridad en este ámbito.

3. IMPLEMENTACIÓN DE LA TEORÍA DE SECURITIZACIÓN AL CASO DE ESTADOS UNIDOS

3.1 ¿Qué es "Estado" y "seguridad"?

El concepto de seguridad ha tenido como referente tradicional los aspectos político-militares desde la constitución de los Estados- nación, en la cual los encargados de la supervivencia del Estados eran el dirigente y sus generales. Esa visión de seguridad fue la base para la corriente más tradicional de las Relaciones Internacionales, el realismo. A medida que el mundo cambió y se diversificó, aparecieron nuevas amenazas que fueron separando esta visión de la realidad. Siendo así, a partir de la crisis de petróleo de los 70´s, los Estados y los estudiosos del sistema internacional entendieron que el concepto de seguridad ya no se podía definir solamente entre el ámbito político militar, estando incorporado a muchos más aspectos.

Para entender como Estados Unidos ha priorizado el ciberespacio como amenaza a su seguridad nacional es necesario entender y explicar conceptos como Estado y seguridad, siendo esta la base para entender los diferentes aspectos de la seguridad nacional.

Buzan hace referencia a la seguridad como una de las razones por la cual se creó el Estado. Se debe tener en cuenta que el "Caos inaceptable se convierte en el motivo por el cual se sacrifica algo de libertad para incrementar los niveles de seguridad, y en este proceso, el gobierno y Estado surgen" (Buzan, 1991). Existen tres teorías (Kantiana, Grociana, Hobbesiana) que explican cómo el Estado suple esta deficiencia de seguridad, sin embargo, en este ejercicio se implementará la teoría de Hobbes (fuente teórica del paradigma realista de las Relaciones Internacionales). Thomas Hobbes empieza por describir el estado de naturaleza en el cual se encontraba la humanidad en sus comienzos. Aquí, el ser humano estaba en una igualdad básica que iba acompañada por una equivalencia en el deseo humano de cumplir con fines, es decir, expectativas frente a la vida. (Hobbes, 1985) Es de esta igualdad que surge el conflicto entre los seres humanos puesto que se crean escenarios en los cuales más de un individuo va a querer lo mismo. En

otras palabras, el ser humano que debe combatir frente a otro para obtener lo deseado se convierte en un competidor para sus semejantes.

Siguiendo lo anterior, Hobbes establece tres condiciones que amplían la lucha entre las personas. La competencia, mencionada anteriormente, rivaliza a los seres humanos y los divide entre aquellos que son una amenaza para los intereses propios y aquellos que no lo son. (Hobbes, 1985) La desconfianza es la segunda característica de este estado de naturaleza que lleva a que el ser humano tome como peligro incluso aquello que no sea una amenaza inminente para su supervivencia.

Por último Hobbes incluye el prestigio, es decir, el deseo de alcanzar una reputación o una posición por encima de sus semejantes como fuente de conflicto. (Hobbes, 1985) Estas tres características son la base para que se dé una constante búsqueda por adquirir más (ya sea material, seguridad, reputación) y esto es directamente contraproducente para la supervivencia de los competidores. Siendo así, la muerte de competidores se convierte en algo positivo y los escenarios donde exista menos competencia son anhelados, por lo cual la muerte se convierte en el principal medio del ser humano para satisfacer sus necesidades. Es así que el Estado de Naturaleza, según Hobbes, se convierte en un estado de guerra incesante y el deseo de supervivencia se establece como imperativo. (Hobbes, 1985)

De acuerdo con Carlos Miranda en su escrito sobre el pensamiento de Hobbes, "todo es válido siempre y cuando se trate de evitar la muerte" (Miranda, 1986). Es en este contexto en el cual "toda acción cuyo fin sea preservar la vida se halla justificada" (Miranda, 1986). Como la preservación es el máximo objetivo, no existen causas justas o injustas, en otras palabras, "las nociones de correcto y de incorrecto, de justicia e injusticia, no tienen allí lugar alguno. Porque donde no existe un poder común, no existe la ley; y donde no hay ley, no hay injusticia" (Miranda, 1986). Se puede entender que para Hobbes los valores, como la justicia, no son inherentes a la condición humana, solo surgieron como resultado del agrupamiento de los seres humanos bajo un poder regulatorio.

Teniendo en cuenta este contexto, en el cual las amenazas son altas y la posibilidad de sobrevivir al enemigo es escasa, se da lugar a la agrupación que hemos denominado a lo

largo de la historia como Estado. El ser humano decide renunciar a parte de su libertad al otorgar poder sobre sí mismo a un ente regulador. Así pues, el hombre cede el derecho natural que tiene sobre su capacidad de preservar su vida al soberano, quien toma ese poder para proteger la totalidad de la población. La manera en que se conforma una sociedad política en la cual se adquieren derechos y responsabilidades es por medio de un pacto o contrato, tanto del soberano como los subordinados. Para poder llevar a cabo su responsabilidad, el soberano impone reglamentos legales que impiden actos en contra de los demás sujetos. Esto se acompaña por el surgimiento de reglamentos morales que se constituyen por medio de conductas y pensamientos socialmente aceptados. Con estas reglas morales y legales se crea una estructura que se conoce como Estado, que por definición se puede considerar como "un cuerpo políticamente soberano organizado por personas usualmente ocupando un territorio definido" (Hobbes, 1985).

De esta manera, el Estado se ha conformado como la unidad más importante y poderosa del sistema internacional. El Estado se convirtió en el parámetro de legitimidad, al cual las demás organizaciones políticas que busquen influenciar y pertenecer al sistema internacional deben asemejarse. Esta legitimidad también se ve reforzada por la particular característica que tiene el Estado, el monopolio de la violencia. Con la capacidad de infligir violencia, el Estado se convierte ahora en el competente e idóneo a la hora de hacer la guerra con otras agrupaciones (Estados) y de regular las acciones de los seres humanos bajo su resguardo. Es de esta manera que el Estado moderno tiene bajo su poder ser garante y protector de su población, territorio, e intereses además de encargado de toda la maquinaria de guerra.

El Estado, como lo definía Webber, es un ente político separado de la sociedad por sus capacidades y funciones. Siguiendo esta línea de pensamiento, Buzan, define el Estado como el "gobierno centralizado" (Buzan, 1991). Buzan complementa esta definición con aquello establecido por Migda:

> El Estado es una organización compuesta por numerosas agencias coordinadas y lideradas por la autoridad ejecutiva que tiene la capacidad de establecer e implementar reglas vinculantes al igual que los parámetros para que otras organizaciones sociales puedan crear reglas (Buzan, 1991).

Como se ha detallado previamente, el Estado es una estructura creada por los seres humanos como mecanismo colectivo para proporcionar la seguridad que no gozarían en un escenario de anarquía. El concepto de seguridad es el eje central tanto de la teoría de Buzan como de la estructura que Estados Unidos ha decidió desplegar frente a las amenazas cibernéticas. Es por esta razón que se debe analizar la diferencia entre seguridad individual y seguridad nacional. La definición de seguridad básica se puede describir como "la ausencia de peligro" o "la ausencia de miedo" (Webster'sDictionary, 2014), sin embargo, se encuentra que esta definición es muy básica para un asunto tan complejo que abarca tantos matices.

La seguridad en su nivel más básico es un asunto del individuo. Es este el que sufre y es afectado en primer lugar por las amenazas que lo rodean. Sin embargo, como este hace parte de una colectividad, estas amenazas se traducen al Estado, el cual es garante de la seguridad del ciudadano. En teoría, en las decisiones de Estado debe primar las necesidades de los seres humanos a los que regula pero en la práctica, es decir en la realidad, somos testigos que eso no siempre aplica. Hemos visto, más de una vez, que la estructura estatal complace a las necesidades de una elite, o un grupo pequeño, que no representa la voluntad de la población en general.

Varios son los ejemplo que Buzan nos da para ilustrar este fenómeno; los más notables son los "Duvaliers en Haití, Boukassa en África Central, Pol Pot en Camboya, Stalin en la Unión Soviética y Hitler en Alemania" (Buzan, 1991). Estos gobiernos tienen la particularidad que se convirtieron en la fuente de amenaza para su propia población.

A raíz de esta diferenciación entre seguridad individual y seguridad estatal, surge el cuestionamiento de cómo se puede llegar a suplir las necesidades y deseos de la población y la estructura estatal a la vez. La historia muestra que es posible tener una congruencia en ambos niveles del Estado, de otra manera la misma idea del Estado sería inconcebible. Esta correspondencia entre intereses es lo que se cataloga como seguridad nacional. Para que pueda existir una seguridad nacional deben existir 3 bases en las cuales se adjuntan los deseos de los ciudadanos y los líderes. El concepto clave en esta situación es nación, dado

que este representa todo aquello que hace del territorio, las instituciones, y la gente, uno solo. El primer componente es "la base física del Estado, en la cual se hace referencia al territorio y la población" (Buzan, 1991). El segundo es la expresión institucional del Estado, es decir, la estructura y componentes institucionales que gobiernan y regulan a los entes físicos. (Buzan, 1991) Por último, se habla de la idea de nación, esta siendo de particular importancia dado que es en la percepción de los ciudadanos que se da legitimidad al funcionamiento de la estructura estatal. (Buzan, 1991)

Estas tres características son, igualmente, la base a la cual todas las amenazas están dirigidas. Todas las amenazas que se constituyen en contra del Estado atacan las instituciones, la población, el territorio, la idea de nación o su legitimidad. La primera condición, la base física, es objeto del mayor número de amenazas, siendo este el campo de batalla y objetivo de guerra tradicional. Aquí están en riesgo la población y el territorio, dentro del cual se encuentra todos los recursos naturales y entes de capital. Este tipo de amenaza es de mayor gravedad y de carácter directo, lo cual ha catapultado la seguridad de este ámbito como la prioridad para los Estados desde su creación.

El segundo tipo de amenazas se dan cuando la estructura institucional está en juego. Existen dos variables que pueden poner en peligro a las instituciones, su integridad física y su legitimidad social. La primera está muy ligada a lo discutido anteriormente cuando se subrayaba el latente peligro que representa la integridad física para la seguridad nacional. (Buzan, 1991) Cuando este es el caso, existe riesgo en que las instituciones sean subyugadas o dominadas por otro ente que no sea el legítimamente establecido. La otra forma de amenaza a las instituciones es por medio de las ideas, es decir, la percepción que se tiene de la legitimidad del Estado. En esta modalidad la amenaza surge cuando las "ideas propuestas y aceptadas por las instituciones no son compartidas por la población y el contexto, y por lo tanto, no gozan de legitimidad" (Buzan, 1991). En este caso las amenazas pueden venir tanto de afuera como dentro del Estado. Es cada vez más frecuente ver casos en que la misma población se levanta en contra de sus dirigentes como resultado de la pérdida de legitimidad. Sin embargo, estas amenazas también pueden venir de afuera, debido al contexto político, económico y social que se presente dentro del sistema

internacional. Ejemplo de esto se pudo ver durante la Guerra Fría, en la cual el mundo se debatía entre las dos líneas de pensamiento que dominaban la política mundial y países como Cuba y Colombia se vieron comprometidos en conflictos internos como resultado de la popularidad del comunismo en América Latina.

Las amenazas a la idea del Estado son las más complejas por que atacan directamente el imaginario de los ciudadanos frente a la estructura Estatal que los gobierna. (Buzan, 1991) Es en este ámbito que la amenaza para los Estados es la fragilidad de su nación. Como se mencionó anteriormente, se trata de establecer qué tan entrelazados están los intereses y necesidades de los ciudadanos y aquellos de la elite dirigente.

En este ámbito, Barry Buzan ofrece modelos en los cuales se determina la fortaleza de la idea de nación de un Estado. El primero es el Nación-Estado, en el cual la nación precede a la formación del Estado y juega un papel importante en su creación. En este caso el Estado se crea con el propósito de suplir las necesidades de la nación y su enlace es fuerte y profundo. (Buzan, 1991) El segundo caso, Estado-nación, se da de forma contraria, el Estado tiene un importante papel en la creación de la nación. (Buzan, 1991) Según Buzan, este modelo de Estado funciona mejor cuando la población del territorio ha sido trasplantada de otra zona y la población existente "no tenga una estructura política y social constituida que permita su desplazamiento"(Buzan, 1991) (ejemplos de este modelo son Estados Unidos y Australia, anteriormente colonias británicas). El tercer modelo es denominado parte Nación-Estado y se da cuando una nación está dividida en varios Estados. (Buzan, 1991) Por supuesto, este modelo no es ideal ya que la nación siempre buscará una estructura estatal que represente la totalidad de la población y el territorio que se considere inherente a la nación.

3.2 ¿Cómo surgen las amenazas?

Al entender que es y cómo se conforma un Estado, es posible analizar cómo se conforman las amenazas. Para esto, existen ciertos sectores o campos en los cuales las acciones que lleven a cabo los individuos y otros países pueden afectar los intereses del Estado. Buzan

delimita este análisis a 5 sectores: político, económico, militar, social y ecológico. (Buzan, 1991)

El sector militar se establece como el sector tradicionalmente más importante. Esto por la sencilla razón que, históricamente, las amenazas militares suelen afectar todos los componentes de un Estado. Los elementos físicos, es decir, el territorio, la población, y elementos de capital, son los directamente afectados en este tipo de amenaza. De igual manera puede destruir físicamente las instituciones y puede debilitar la idea de Estado. Las amenazas militares pueden variar en su carácter, unas siendo menores y específicas, como los *hackivistas* que buscan interrumpir el funcionamiento de páginas oficiales para mandar un mensaje, mientras que otras son generales, como la desactivación de la red nacional de electricidad de un país.

En el sector político, las amenazas van dirigidas a dos componentes: la idea de Estado y la estabilidad de la institucionalidad del Estado. (Buzan, 1991) Su objetividad, como ha sido una constante en otros sectores, puede ser menor o generalizada. De igual manera, las fricciones pueden venir dentro del Estado, de presión de grupos extranjeros, o Estados que ven afectados sus propios intereses. Acciones leves se puede describir como la presión de un grupo de la sociedad por llevar a cabo políticas que beneficien sus intereses. Acciones destinadas a un efecto más general tienden a buscar un gran cambio como el creado "al derrocar un gobierno, fomentar separatismo, e interrumpir el diálogo o concordancia entre los intereses de la población y las acciones del gobierno"(Buzan, 1991).Las amenazas políticas son tan peligrosas en Estados débiles como en Estados fuertes ya que la estabilidad política es fácilmente afectada cuando los problemas vienen de adentro. (Buzan, 1991) Colectividades como los *indignados* o *anónimos* (críticos de la estructura política, económica y social actual)deben su popularidad en todo el mundo a las redes sociales que han facilitado el intercambio de información a nivel mundial. Este ejemplo describe cómo el ciberespacio puede servir como medio para que ciertos actores afecten la estabilidad política de un Estado.

El sector político es particularmente importante en los Estados fuertes, como Estados Unidos, ya que a pesar de su gran capacidad militar, de poco le sirve su armamento

cuando el descontento viene de su propia población. En este contexto, la diversidad de pensamiento e ideas deben ser respetadas dentro de un fino equilibrio que también pide que el gobierno limite las expresiones extremistas que puedan ser generadoras de divisiones. Es este frágil equilibrio el que debe manejar el Estado puesto que, por un lado, debe garantizar los derechos de los ciudadanos y por otro lado debe evitar que ideologías organizadas tomen la suficiente fuerza como para retar la estabilidad y legitimidad del gobierno. Por último, se puede distinguir entre las amenazas intencionales y aquellas que surgen como efecto de cambios estructurales. Las numerosas intervenciones de Estados Unidos en asuntos domésticos de otros países demuestra que algunas amenazas son intencionales, llevadas a cabo por un país que ve sus intereses comprometidos con las acciones y conjeturas que se dan en otros países.

Es así que las intervenciones en Corea e Iraq marcaron el tipo de política exterior intervencionista de Estados Unidos durante el siglo XX y XXI. A diferencia de lo anterior, existen amenazas estructurales, las cuales surgen como resultado de conjeturas del contexto. Ejemplo de esto es la primavera árabe que comenzó en Túnez, como resultado del descontento social y político que se daba en su interior. Este ánimo revolucionario se propagó fuertemente en los demás países Árabes del norte de África y países como Egipto y Libia pronto se encontraron en una situación similar a Túnez.

El tercer sector donde pueden surgir amenazas para el Estado es la sociedad. Buzan, en su libro *People, States, and Fear* describe la seguridad social como la "sostenibilidad, bajo condiciones aceptables de evolución, de los patrones tradicionales de lenguaje, religión, etnia, costumbres y cultura" (Buzan, 1991). Estas amenazas suelen venir del interior del Estado, por lo cual se debe manejar un delicado equilibrio entre suprimir identidades sub-nacionales, homogeneizar la población dentro de los parámetros tradicionales y el respeto a los derechos individuales de cada ciudadano. Tradicionalmente, las amenazas a estos valores suelen ser domésticas, pero en un mundo globalizado, las amenazas pueden venir de afuera también. La influencia que puede tener un grupo con estructuras de pensamiento organizadas en un país foráneo puede ser alta dado los numerosos medios de comunicación y contacto que existen actualmente.

Otro sector dentro del Estado que afecta por igual a la población como a la estructura gubernamental y política, es la economía. Según Buzan, "las amenazas económicas son, sin duda alguna, las más difíciles y confusas para tratar dentro del marco de seguridad nacional" (Buzan, 1991). Esto debido a la misma naturaleza del sistema de mercados en la cual el riesgo, competencia, agresividad e incertidumbre son partes inevitables para aquellos que accionan en economías de mercado. (Buzan, 1991) A pesar de estas características un tanto negativas, el sistema económico que conocemos es bastante eficiente siendo su longevidad fiel testigo de este fenómeno. Aunque ha habido momentos en los cuales el sistema económico muestra falencias, también ha demostrado ser un mecanismo eficiente en la distribución, producción, innovación, y crecimiento de los recursos globales. (Buzan, 1991) A esta dinámica riesgosa se añade que el Estado es un actor más del mercado y no goza de habilidades exclusivas puesto que al Estado se suman los individuos, grupos, compañías, bancos y demás Estados. Tanto la naturaleza del mercado como la multiplicidad de actores hacen que las acciones de los Estados no tengan la influencia que gozan en otros sectores. Este sector es tal vez el más riesgoso en cuanto al ciberespacio dado su alto grado de dependencia a la tecnología informática. La bolsa de valores, el intercambio de acciones y dinero, y la promulgación de información de este sector se da primordialmente en el ciberespacio. De esta manera, un ataque a la red de las diversas bolsas de valores del mundo puede tener como resultado una crisis económica sin precedentes.

El último sector, según Buzan, en el que pueden surgir amenazas en contra del Estado es el ecológico. En el sector ecológico, al igual que el sector militar, se ve afectado, en principio, el aspecto físico del Estado. La importancia de este sector ha incrementado en los últimos años en gran parte por la expansión e inmediatez con que se da el conocimiento. En 2010, cuando se produjo un derrame petrolero en el Golfo de México, el mundo entero estaba pendiente de los daños ambientales que produjo. Adicionalmente, los desastres ecológicos no siempre se limitan a las fronteras estatales, lo cual convierte un derrame petrolero, polución ríos contaminados en problemáticas nacionales e internacionales.

3.3 La securitización del ciberespacio por parte de Estados Unidos

Con tantas amenazas, es evidente que los Estados deben crear una estructura que organice las amenazas de leves a graves. Esto se hace por medio del proceso de securitización, por el cual el gobierno expone lo que ellos consideran y necesitan elevar ante la población como amenazas latentes. Securitización se debe entender como un tema, presentado como una amenaza existencial a un objeto de referencia designado, que tiene como fin la justificación del uso medidas extraordinarias para manejar la amenaza. (Buzan,Waever y Wilde, 1998) El proceso de securitización, como lo describe Barry Buzan y Ole Waever, cuenta con ciertos pasos o características condicionales.

Para la Escuela de Copenhague, la securitización se basa en un supuesto principal: "la enunciación de la seguridad en sí crea un nuevo orden social en el que 'la normalidad política ' se basa en aquello que indica el actor regulador" (Oxford bibliographies, 2014). Las características a las cuales se hacía alusión anteriormente, se hacen necesarias en el proceso de securitización dado la importancia de la relación locutor- audiencia. La primera característica tiene que ver con la lingüística, aquella serie de palabras que se escogen cuidadosamente para poder emitir un mensaje. Este imperativo hace referencia a la importancia de las palabras, sus diferentes significados y cómo cambia su relevancia dependiendo del contexto. (Buzan,Waever y Wilde, 1998) La segunda característica tiene que ver con el contexto, lugar y tiempo en el cual se quiere dar ese mensaje. Este contexto también incluye a los particulares, es decir, aquellos que reciben el discurso securitizador del gobierno. Buzan afirma que "las personas particulares y circunstancias de un caso determinado deben ser apropiados para la realización del procedimiento invocado" (Buzan et al, 1998). Thierry Balzacq igualmente da una visión que complementa aquello postulado por Buzan, Waever, y Jaap de Wilde en su libro *Security: A New Framework forAnalysis*; Balzacq dice que esta estructura no es rígida puesto que "se entiende mejor como una práctica estratégica (pragmática) que ocurre en el interior, y como parte de un configuración de las circunstancias, incluido el contexto, disposición del público, y el poder tanto del que habla como el que escucha" (Balzacq, 2005).

Invocar la seguridad ha sido el medio para legitimar el uso de la fuerza y la movilización de los actores y recursos del Estado en un fin concreto. Este proceso es la suma de esfuerzos diplomáticos, discursos, documentos publicados, declaraciones de oficiales de alto rango, e incluso estudios académicos de entidades del Estado y universidades asociadas. En el caso específico de Estados Unidos, se puede ver un proceso que se basa inicialmente en la publicación de documentos oficiales que hacen referencia al ciberespacio. Estos documentos tuvieron alta resonancia en los medios de comunicación y ellos se encargaron de difundir la información a la población general. A esto le acompañó un auge en la investigación y publicación académica de universidades estadounidenses y el mundo.

Es importante resaltar que securitización hace necesario un trabajo de persuasión por parte del ente regulador, para así lograr convencer al público que la amenaza a la que se alude tiene un carácter de peligro inminente. Eso es precisamente lo que llevó a cabo el presidente Bush y después, a manera de consolidación, el Presidente Obama. Los primeros informes sobre la seguridad cibernética datan del 2001, en los que se hace un llamado a los ciudadanos estadounidense para que entiendan que el ciberespacio no es solo un medio de comunicación y entretenimiento ya que también se consolidó como un medio por el cual un sin número de enemigos pueden llevar a cabo diferentes tipos de ataques. Para el 2003 se hacen públicos los numerosos ataques a páginas de entes públicos y privados ligados con la seguridad de Estados Unidos. El uso mediático de estos ataques abrió campo para que el pueblo, receptor de la agenda securitizadora del Estado, viera como esta amenaza se traducía a realidad.

A partir del 2003, se da la publicación de la primera estrategia nacional para asegurar el ciberespacio durante administración Bush. En este documento se hace por primera vez alusión al propósito de concientizar a la población general sobre las amenazas del ciberespacio además de entrenar y educar a funcionarios para que puedan suplir las necesidades de la seguridad cibernética. (Department of Defense, 2003) Este documento tuvo como gran aporte que por primera vez el gobierno hablaba de crear un sistema de respuesta nacional para el ciberespacio (anteriormente se hablaba de un plan, no de un

sistema físico y concreto), dentro de este sistema se propone "ampliar la red de información y advertencia de ciberespacio para apoyar el papel de DHS en la coordinación de la gestión de crisis de la seguridad del ciberespacio" (Department of Defense, 2003), lo cual plantea que otras agencias y departamentos se involucren en la gestión de asegurar el ciberespacio.

En 2005, el comité de apoyo presidencial en asuntos de tecnologías de información publicó un estudio en el cual detalla las deficiencias en la defensa de Estados Unidos, y propone ciertas normas a seguir para el gobierno en este tema. El documento se centra en la priorización que debe hacer el Estado en la ciberseguridad para así poder llevar a cabo regulaciones en el tema. Además, el Comité advierte que se debe dar la priorización para que se pueda dar lugar a la institucionalización de la amenaza, es decir, la creación de instituciones y organismos encaminada a suplir la seguridad en el ámbito cibernético. Su priorización, según este documento, facilitaría la posibilidad de un mayor presupuesto dirigido a enfrentar esta amenaza. El comité por fin señala la desventaja que se tiene cuando la población general no tiene conocimiento de la amenaza.

Los documentos que el gobierno ha publicado no son el medio preciso para llevar a cabo un proceso de securitización dado que la mejor manera de transmitir un mensaje es por medio de declaraciones puntuales de actores relevantes (alto nivel). Así pues, varios altos funcionarios de Estados Unidos han dado declaraciones acerca de las amenazas del ciberespacio, de las cuales se detallarán algunas.

Según Alan Paller, director del SANS Institute, los problemas de Estados Unidos frente a las amenazas del ciberespacio son varios. El principal problema radica en la dependencia que tiene Estados Unidos del internet, que según él, es más alta que sus adversarios (UnitedStatesSenate, 2002). El Almirante Haney, Comandante del Comando Estratégico de Estados Unidos, declaró que se vive actualmente un entorno de seguridad complejo, "dinámico e incierto" (SenateCommitteeOnArmedServices, 2013). En su testimonio ante el congreso, Haney añadió que los avances militares de aire, tierra, y "dominios- como el espacio y ciberespacio" (SenateCommitteeOnArmedServices, 2013) han complejizado la capacidad de Estados Unidos para mantener su ventaja comparativa frente a otros Estados y actores no estatales. Como ex jefe de la NSA, el general Alexander

también dijo "...los acontecimientos cibernéticos han cambiado de naturaleza, antes iban direccionados a la explotación, ahora buscan la interrupción del funcionamiento y, finalmente, los ataques resultaran en de la destrucción física" (SenateCommitteeOnArmedServices, 2013).

El discurso del Presidente Barack Obama sobre ciberseguridad en Mayo del 2009 es tal vez el más significativo en el proceso de securitización. En esta ocasión el presidente empezó resaltando la importancia de la infraestructura digital de Estados Unidos como "la columna vertebral que sostiene una economía próspera y un ejército fuerte y un gobierno abierto y eficiente. Sin esa base no podemos hacer el trabajo" (Whitehouse, 2009). Tras resaltar la importancia de la era digital, Obama añade:

> Durante mucho tiempo se ha dicho que los cambios en las comunicaciones y la tecnología de la información han dado a luz a un mundo virtual. Pero no nos engañemos: Este mundo - el ciberespacio - es un mundo del cual dependemos todos los días. Es nuestro hardware y nuestro software, nuestros ordenadores y portátiles y los teléfonos celulares y Blackberries que se han tejido en cada aspecto de nuestras vidas. Son las redes de banda ancha por debajo de nosotros y las señales inalámbricas que nos rodean, las redes locales en nuestras escuelas y hospitales y empresas, y las redes masivas que alimentan nuestra nación. Son las redes militares y de inteligencia que nos mantienen a salvo, y la World Wide Web que nos ha interconectado más que en cualquier momento en la historia humana (Whitehouse, 2009).

A partir de este pequeño fragmento del discurso se puede evidenciar que se busca aproximar la amenaza con aquellas actividades que son familiares a los ciudadanos al mencionar varios objetos que se usan diariamente, vitales para la vida normal de cualquier norteamericano, mostrando así que cada uno de estos aparatos tecnológicos puede servir como puente para un ataque en contra de la población. Adicionalmente, el presidente Obama también nombra varios lugares esenciales para la vida moderna, escuelas, hospitales y empresas para hacer sentir al receptor que esta amenaza se envuelve en todos los ámbitos de la vida. Al acercar la amenaza a los espacios habituales de cualquier ciudadano, el discurso hace que la audiencia perciba la amenaza como latente e incluso inminente.

El presidente Obama también buscó acentuar la amenaza informática a dos realidades de la población, la economía y la sociedad. A continuación un pequeño fragmento del discurso en el que se logra enaltecer estos dos sectores como los más afectados por la inseguridad cibernética:

> Nos apoyamos en el internet para pagar nuestras cuentas, ir de compras, para presentar nuestros impuestos. Pero hemos tenido que aprender todo un nuevo vocabulario sólo para mantenernos a la vanguardia de los criminales cibernéticos que quieren hacernos daño - spyware y malware y suplantación de identidad y botnets. Millones de estadounidenses han sido víctimas, su privacidad violada, sus identidades robadas, sus vidas perturbadas, y sus billeteras vaciadas. Según una encuesta, en los últimos dos años el crimen cibernético le ha costado a los estadounidenses más de $ 8 mil millones (The White House, 2009).

Tras detallar qué sectores serían los más afectados, Obama introduce la finalidad real del discurso, es decir, la securitización por medio de lingüística, que define la amenaza, los agentes reguladores, y los pasos a seguir:

> Esto es también una cuestión de seguridad nacional. Contamos con las redes de computadoras para entregar nuestro petróleo y gas, nuestro poder y nuestra agua. Contamos con ellos para el transporte público y el control del tráfico aéreo" (Whitehouse, 2009).

Sin duda alguna, los grupos terroristas son la amenaza priorizada en Estados Unidos en el siglo XXI como resultado de los ataques del 11 de septiembre. Por esta relevancia, Obama relaciona estas dos amenazas al mencionar en este discurso que "Al Qaeda y otros grupos terroristas han hablado de su deseo de dar rienda suelta a un ataque cibernético en nuestro país - los ataques que son más difíciles de detectar y difícil de defender" (Whitehouse, 2009), "…el mundo actual, los actos de terror podrían provenir no sólo de unos pocos extremistas con chalecos suicidas, sino de unas pocas pulsaciones de teclas en el ordenador - un arma de perturbación masiva" (Whitehouse, 2009).

Por último, el gobierno estadounidense muestra lo que será su plan de acción para el futuro cercano por medio de la frase más importante de la totalidad del discurso. El presidente de Estados Unidos finaliza diciendo: "puedo anunciar que mi administración buscará un nuevo enfoque integral para asegurar la infraestructura digital de Estados Unidos" (Whitehouse, 2009). En esta corta y muy diciente frase, el presidente muestra la intención de una regulación rápida y diferente de lo que se había hecho hasta ahora. Su claro propósito es elevar esta amenaza en su agenda y crear cambios claros y contundentes. Él añade que:

> Se debe dar a estos esfuerzos (de regular el ciberespacio) el enfoque de alto nivel y la atención que se merecen. Como parte de la agenda de Seguridad Nacional, anunció esta semana que - Estoy creando una nueva oficina aquí en la Casa Blanca, que será dirigida por la Coordinadora de ciberseguridad. Debido a la importancia crítica de este trabajo, yo personalmente seleccione este funcionario. Voy a depender de este funcionario en todos los asuntos relativos a la seguridad cibernética, y este funcionario tendrá todo mi apoyo y el acceso regular a mí mientras nos enfrentamos a estos retos. Para asegurar la rendición de

> cuentas en las agencias federales, la seguridad cibernética será designada como una de mis prioridades clave de la gerencia. Hitos claros y actuaciones métricas medirán el progreso (Whitehouse, 2009).

El ciberespacio también ha sido tema relevante en varios de los discursos del *Estado de la Unión*, este discurso anual marca el camino que seguirá cada gobierno para el siguiente año, además de enumerar los logros del año inmediatamente anterior. En su discurso de 2011, Obama centró su discurso en las tecnologías informáticas y cómo estas se incorporan en los demás aspectos de la vida y seguridad de los ciudadanos estadounidense. Siendo así, el Presidente de los Estados Unidos declaró que "las reglas han cambiado. En una sola generación, la revolución tecnológica ha transformado la manera en que vivimos, trabajamos y hacemos negocios" (TheWhitehouse, 2011). Pero también añadió que Estados Unidos no está solo en esta nueva era digital ya que existen países a la vanguardia de las tecnologías informática como:

> China e India, que se dieron cuenta de que con algunos cambios propios, podían competir en este nuevo mundo. Y así empezaron a educar a sus hijos antes y por más tiempo, con mayor énfasis en matemáticas y ciencias. Están invirtiendo en investigación y nuevas tecnologías. Recientemente, China se convirtió en el hogar de instalaciones de investigación solar más grande del mundo privado, y el ordenador más rápido del mundo (TheWhitehouse, 2011).

En esa oportunidad, el presidente puso énfasis en lo que el gobierno consideraba los generadores de una futura superioridad informática frente a otros Estados. Es por esta razón que el énfasis era la economía y la educación, ambas necesarias para fomentar el estudio de la informática en los centros académicos que formarían expertos informáticos esenciales para la securitización del ciberespacio. Para esto Obama finaliza su discurso de la siguiente manera:

> El primer paso para ganar el futuro es alentado la innovación estadounidense. Hace treinta años, no podíamos saber que algo llamado internet llevaría a una revolución económica. Lo que podemos hacer - lo que Estados Unidos hace mejor que nadie - es la chispa de la creatividad y la imaginación de nuestra gente. Somos la nación que pone coches en las calzadas y las computadoras en las oficinas; la nación de Edison y los hermanos Wright; de Google y Facebook. En Estados Unidos, la innovación no se limita a cambiar nuestras vidas. Es cómo nos ganamos la vida. Mantener nuestro liderazgo en investigación y tecnología es crucial para el éxito de los Estados Unidos. Pero si queremos ganar el futuro - si queremos que la innovación produzca empleos en Estados Unidos y no en el extranjero - entonces también tenemos que ganar la carrera para educar a nuestros hijos (TheWhitehouse, 2011).

En 2012, Obama incorporó el ciberespacio en su discurso desde el ámbito militar señalando que:

> Trabajando con nuestros líderes militares, he propuesto una nueva estrategia de defensa que garantiza que mantenemos las mejores fuerzas armadas del mundo, mientras que el ahorro de casi medio billón de dólares en nuestro presupuesto. Para estar un paso por delante de nuestros adversarios, ya he enviado legislación al Congreso para que asegure a nuestro país de los crecientes peligros delas ciberamenazas (TheWhitehouse, 2012).

En el discurso de *Estado de la Unión* de 2013, se mencionan los diferentes tipos de amenazas que surgen del ciberespacio mientras que se propone una nueva estrategia para su regulación. El presidente enfatiza que:

> Estados Unidos debe hacer frente a la creciente amenaza de los ciberataques. Ahora, sabemos que hackers roban identidades de las personas y se infiltran en los correos electrónicos privados. Sabemos que países y empresas extranjeras sustraen nuestros secretos corporativos. Ahora nuestros enemigos también están buscando la posibilidad de sabotear nuestra red eléctrica, nuestras instituciones financieras, nuestros sistemas de control de tráfico aéreo. No podemos mirar hacia atrás a partir de ahora y me pregunto por qué no hicimos nada frente a amenazas reales a nuestra seguridad y nuestra economía (TheWhitehouse, 2013).
>
> Por eso, el día de hoy, he firmado una nueva orden ejecutiva que fortalecerá nuestras defensas cibernéticas aumentando el intercambio de información, y el desarrollo de normas para proteger nuestra seguridad nacional, nuestros empleos y nuestra privacidad. Pero ahora el Congreso debe actuar, por la aprobación de leyes para dar a nuestro gobierno una mayor capacidad para proteger nuestras redes y disuadir los ataques (TheWhitehouse, 2013).

El siguiente paso en la securitización (después de transmitir el mensaje propuesto) es especificar aquellos actores que puedan convertirse en amenaza. En esto, Estados Unidos ha sido enfático en mostrar a China como el principal enemigo en este tema. Cada año, el gobierno Estadounidense publica el Informe Anual del Departamento de Defensa al Congreso que describe la capacidad militar de China y en el cual se hace énfasis especial en las capacidades cibernéticas de esta potencia asiática. La primera referencia que se tiene de capacidades cibernéticas se plasmó en el Informe de 2001 donde se detalló la gran estrategia militar China, que incluía la modernización de su tecnología informática para uso militar.

Así, altos representantes de Estados Unidos han declarado al gobierno chino en numerosas ocasiones como autor de ataques cibernéticos con la finalidad de llevar esta amenaza a un nivel más real, más cercano a la población, por medio de la consolidación de una figura que represente esta amenaza. Las declaraciones de funcionarios como Allan Paller, director del Instituto SANS que señaló que los ataques fueron rastreados hasta la provincia de Guandong, China, han sido fundamentales para que los ataques de Titan Rain sean relacionados con el ejército Chino. De manera más directa, el gobierno de Barack

Obama acusó explícitamente (en el Informe Anual al Congreso sobre las capacidades militares de China) al gigante asiático de ataques contra los sistemas informáticos del gobierno estadounidense y contratistas de defensa, diciendo que la finalidad sería mapear "las capacidades militares que podrían ser explotadas durante una crisis" (U.S Congress, 2013).

Aun sin haber hecho público algún tipo de prueba concreta, oficiales del gobierno estadounidense daban su apoyo a la teoría que se manejaba en los medios, que culpa a China de gran parte de los cuantiosos ataques. Se han hecho numerosos estudios y artículos tanto del gobierno estadounidense como de los medios de comunicación con referencia a la estructura militar de China y su contraparte estadounidense. Al hacer esta comparación, los medios y el mismo gobierno promovieron un balance desalentador al asumir una deficiencia organizacional e institucional frente a China.

Es de esta manera que se puede concluir que es a partir de la securitización que Estados Unidos ha podido priorizar ciertas amenazas por encima de otras. Tal como lo hizo con el terrorismo, a partir del 2001 y después con el ciberespacio. En este proceso se hizo uso de discursos presidenciales, declaraciones de funcionarios de alto nivel, declaraciones de oficiales militares de alto rango, publicación de documentos concernientes al peligro del ciberespacio, y documentos oficiales que reflejan la fragilidad de la infraestructura y debilidad de la defensa de Estados Unidos en este ámbito. A esto se suma los reportes anuales sobre la capacidad militar de China, en el cual se da un espacio especial a sus capacidades cibernéticas.

A través de estos medios, el gobierno de Estados Unidos hizo público su intención de priorizar el ciberespacio al considerarlo una amenaza a su seguridad nacional. Es a través de este proceso que Estados Unidos puede empezar a crear instituciones, cargos oficiales, y leyes regulatorias encaminadas a cambiar el ambiente anárquico del ciberespacio. Estos procesos han sido exitosos en la medida en que la población ha aceptado esta priorización del ciberespacio y lo percibe como una amenaza latente en su contra.

4. CONCLUSIONES

El ciberespacio se ha conformado como un ámbito importante en las sociedades del Siglo XXI ya dio lugar a una mayor interconectividad e intercambio de información. Sin embargo, como se ha expuesto a lo largo de este documento, este espacio también da lugar a un nuevo tipo de amenazas. Como respuesta al surgimiento de nuevas amenazas, Estados Unidos llevó a cabo un proceso de securitización. De este proceso se puede concluir lo siguiente:

Primero, basado en lo visto a lo largo de este trabajo, se puede determinar que los ataques cibernéticos en contra de Estados Unidos fueron importantes a la hora de reforzar el discurso que ha manejado su administración (Bush, Obama) respecto a la inseguridad del ciberespacio. Aunque el gobierno ya expresaba su intención de priorizar el ciberespacio como una amenaza para Estados Unidos, solo es hasta 2003 que este fenómeno resultó relevante para los medios de comunicación y en la academia nacional e internacional, es en este año cuando se dan a conocer los ataques denominados "Titan Rain" por el ejército estadounidense.

Cuando los medios de comunicación expusieron otros casos de ataques cibernéticos, se encontró que más oficiales de alto rango daban declaraciones acerca de este tema. Es también después del 2003 que se empiezan a generar acciones regulatorias por parte del gobierno en la medida en que buscó crear instituciones y leyes enfocadas en el manejo de la seguridad en este nuevo contexto. De esta manera, una vez analizada la problemática es posible sostener que la hipótesis es válida por cuanto los ataques sí influenciaron el proceso de securitización de Estados Unidos. Sin embargo, hay que enfatizar que los ataques no fueron causa de la securitización sino complemento a esto proceso en la medida en que influenciaron la percepción de aquellos que recibían el discurso securitizador e hicieron que esta amenaza se percibiera como real y latente.

Segundo, se puede concluir que la teoría de securitización, desarrollada por Barry Buzan, con aportes de Ole Waever y Jaap de Wilde, está vigente y sirve como una herramienta para interpretar y entender la realidad internacional. Esta teoría fue un medio

para entender por qué los Estados deciden regular ciertas amenazas entre las millones que existen en la actualidad. También es importante para entender cómo se lleva a cabo el proceso de securitización, cuáles son los factores de una securitización exitosa, y cuáles son los efectos de este proceso.

Tercero, en el caso puntual de Estados Unidos que se ha analizado bajo la visión de la securitización de Buzan, se llegó a una conclusión. Basado en lo precisado a lo largo del trabajo, es factible decir que el proceso de securitización en Estados Unidos se dio en la medida en que la población aceptó el ciberespacio como un medio en el cual se materializan numerosas tipos de amenazas (se logró cambiar la perspectiva que se tenía); De igual manera, la comunidad internacional también ha mostrado su apoyo en la medida en que este tema se ha priorizado en las agendas de otros Estados (China, Rusia, Unión Europea siendo los más pertinentes) y en la agenda de organizaciones internacionales como la OTAN, la OEA y Naciones Unidas.

Cuarto, teniendo en cuenta todo lo descrito en este trabajo se puede decir que la securitización del ciberespacio será mucho más compleja que los procesos llevados a cabo en otros campos estratégicos (mar, tierra, aire) dado que es un invento humano que está sujeto a reglas diferentes a las naturales. Un ejemplo actual es China, país que ha tratado de regular el internet pero esto no ha sido del todo exitoso ya que los ciudadanos cambian de servidor de red (a uno fuera de China) para acceder a las páginas (facebook, youtube) vedadas. El proceso de China muestra la complejidad que acompaña el ciberespacio, lo cual hará su regulación objeto de debate entre los diferentes sectores de la sociedad (población, gobierno, empresas).

Por último, se puede pronosticar que la regulación del ciberespacio va tomar más importancia en los años que vienen, en la medida en que más países se unirán en esta causa. Esto es posible gracias a los países con mayor influencia (potencias como Estados Unidos, China, Rusia, China, Alemania, entre otros) que ya han priorizado esta amenaza en su agenda y, como se mencionó antes, numerosas organizaciones internacionales también.

Los procesos más notorios son los que han llevado a cabo la OTAN, OEA, y Naciones Unidas que tienen como prioridad la concientización de la población y la

seguridad de sus propias redes y páginas. Sin embargo, este tipo de procesos dan solo un vistazo a lo que será el enfoque del ciberespacio en el futuro, donde la regulación no será asunto individual del Estado, y probablemente se regulará (como se ha hecho con las grandes amenazas hasta ahora) por medio de complejos de seguridad.

BIBLIOGRAFÍA

Buzan, B. (2008). *La gente, los Estados, y el miedo*. Colorado: Lynne Rienner Publishers.

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

Clarke, R, Knake, R. (2009). *Cyberwar: The next threat to national security and what to do about it*. New York: Harper Collins

Denning, D. (1998). *Information Warfare and Security*. Boston, MA: Addison Wesley

Dunn, C. (2008). *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age*. London: Routledge

Libicki, M. (1997).*Defending Cyberspace*. Washington D.C: National Defense University

MIT. (1998). *Democracy and Cyberspace: First Principles*. Massachusetts: MIT's conference on Democracy and Digital Media

National Research Council. (2010). *Letter Report from the Committee on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy*. Washington D.C: National Academies Press

Nye, J. (2004). *Power in the Global Information Age: From Realism to Globalization*. London: Routledge

Waever, O. (1998). *Securitization and Desecuritization*. New York, Columbia University Press

Capitulos de libro

Hobbes, T. (1985). Of the first and second natural laws, and of contracts. En: *Leviathan.* (59-65). Oregon: Penguin Book

Hobbes, T. (1985).Of the natural condition of Mankind, as concerning their felicity, and misery.En: *Leviathan*. (56-59)Oregon: PenguinBook

Artículos en publicaciones periódicas académicas

Balzacq, T. (2005). The Three Faces of Securitization: Political Agency, Audience and Context. *European Journal of International Relations.* 11 (2), 171-201. Disponible en: http://ejt.sagepub.com/content/11/2/171.short?rss=1&ssource=mfc

Buzan, B. (1991). New Patterns of Global Security in the Twenty-First Century.*International Affairs*. 67 (3), 431- 451. Disponible en: http://www.jstor.org/discover/10.2307/2621945?sid=21105894502313&uid=4&uid=2

Buzan, B. (2006). Will the ‘global war on terrorism’ be the new Cold War? *International Affairs*.82 (6), 1101- 1118.

Buzan, B, Waever, O. (2009). Macrosecuritisation and securityconstellations: reconsidering scale insecuritisation theory.*International Studies*. 35, 253–276

McDonald, M. (2008).Securitization and the Construction of Security.*European Journal of International Relations*. 14 (4), 563–587. Disponible en: http://ejt.sagepub.com/content/14/4/563.short

Metzl, J. (2001). Network diplomacy.*Georgetown Journal of International Affairs*.77 (2). Disponible en: http://carnegieendowment.org/2001/04/01/network-diplomacy/

Miranda, C. (1986). Realismo e idealismo en el estudio de las relaciones internacionales: la influencia de Hobbes y de Kant. *Revista Ciencia Política*. 8 (1), 88-100. Disponible en: www7.uc.cl/icp/revista/pdf/rev812/ar3.pdf

Orozco, G. (2006). El aporte de la Escuela de Copenhague a los estudios de seguridad. Fuerzas Armadas y Sociedad. 20 (1). 141-162

Artículos en publicaciones periódicas no académicas

Chinese hackers promptNavycollegesiteclosure. (2005). *Washington Times.*Disponible en: http://www.washingtontimes.com/news/2006/nov/30/20061130-103049-5042r/?page=all

Graham, B. (2005).Hackers attack via chinese web sites. *Washington Post*. Disponible en: http://www.washingtonpost.com/wpdyn/content/article/2005/08/24/AR2005082402318_2.html

Thornburgh, N. (2005). *The invasion of the Chinese cyberspies*.Time Magazine Disponible en: http://courses.cs.washington.edu/courses/csep590/05au/readings/titan.rain.htm

Wo Lap Lam, W. (2003). China army looks to technology. *CNN International.* Disponible en: http://edition.cnn.com/2003/WORLD/asiapcf/east/03/09/china.generals/index.html

Otros

Billo, C, Chang, W. (2004). Cyber Warfare. *Institute for Security Technology Studies At Dartmouth College*. Disponible en: www.ists.dartmouth.edu/docs/execsum.pdf

Ciclo de vida de un virus. (2013). *Universidad Autónoma de Yucatán.*Disponible en: http://www.uady.mx/~teleinfo/virus/ciclo.php

Computer term definitions. (2013). Pop up definition. *Webopedia.* Disponible en: http://www.webopedia.com/TERM/P/popup_ad.html

Computer Histoy Museum.(2012). Information Age.*Computer History Museum.*Disponible en: http://www.computerhistory.org/

Definitions: Security. (2014). Disponible en: http://www.merriam-webster.com/dictionary/ *Webster's Dictionary* security

Department of Defense.(2011). Department of defense strategy for operating in cyberspace.Disponible en: http://www.defense.gov/news/d20110714cyber.pdf

Department of Defense (2010).U.S. Cyber Command Fact Sheet.Disponible en: http://www.defense.gov/home/features/2010/0410_cybersec/docs/CYberFactSheet%20UPDATED%20replaces%20May%2021%20Fact%20Sheet.pdf

Department of Defense.(2003). the national strategy to secure cyberspace.Disponible en: https://www.uscert.gov/sites/default/files/publications/cyberspace_strategy.pdf

Department of Homeland Security (2013). What is critical infrastructure?.Disponible en: http://www.dhs.gov/what-critical-infrastructure

Department of Homeland Security.(2001). Executive Order 13231, 2001.Disponible en: https://www.dhs.gov/.../executive-order-13231-dated-2001-10-16-initial

Department of Homeland Security.(2014). National Critical Infraestructure.Disponible en: http://www.dhs.gov/critical-infrastructure-sectors

Department of Transportation.(2013) Federal alert system.Disponible en: http://www.ops.fhwa.dot.gov/publications/fhwahop05029/chapter_1.htm

Deparment of Treasury (2013).Bureau of Consumer Financial Protection report.Disponible en: http://www.treasury.gov/initiatives/Pages/cfpb.aspx

Establishment of U.S. Army Cyber Command.(2013). *Army Cyber Command Homepage*. Disponible en: http://www.arcyber.army.mil/history.html

Ellis, J, Fisher, D, Longstaff, T, Pesante, L, Pethia, R. (1997). Infrastructure protection. *Carnegie Mellon University*. Disponible en: resources.sei.cmu.edu/library/asset-view.cfm?assetid=12731

Federation of American Scientists.(2014). Information Warfare.*Federation of American Scientists*.Disponible en: http://www.fas.org/irp/world/china/docs/iw_wang.htm

GovTrack. (2013). H.R. 624: Cyber Intelligence Sharing and Protection Act. Disponible en: https://www.govtrack.us/congress/bills/113/hr624

GovTrack. (2012).H.R. 3523 (112th): Cyber Intelligence Sharing and Protection Act. Disponible en:https://www.govtrack.us/congress/bills/112/hr3523

GovTrack. (2011). S. 3414 (112th): CSA. Disponible en: https://www.govtrack.us/congress/bills/112/s3414

International crime complaint center. (2014). IC3 Annual Crime Report. Disponible en: http://www.ic3.gov/media/annualreports.aspx

Internet Society. (2014). Whatis Internet?.*Internet History.* Disponible en: http://www.internetsociety.org/internet/what-internet

IP Commission. (2013). IP Commission Report. Disponible en: http://www.ipcommission.org/report/IP_Commission_Report_052213.pdf

Library of Congress.Congressional Research Service Report for Congress. 2007. Disponibleen:http://fpc.state.gov/c18185.htm

Mandiant.(2013). Mandiant Report APT1.*MandiantCybersecurity Firm*.Disponible en: intelreport.mandiant.com

Navy Force (2013).*About the Navy Cyber Forces*. United States Navy Homepage Disponible en: http://www.cyberfor.navy.mil/

Norton Advisor.(2014). Computer Virus History.Norton AdvisorCompany. Disponible en: http://www.nortonadvisor.com/knowledge-center/computer-virus-history.html

Organización de los Estados Americanos. (2012). Declaration strengthening cyber-security in the americas. Disponible en: http://www.oas.org/cyber/documents/Declaration.pdf

Organización de los Estados Americanos. (2013). Cyber Security Program. Disponible en: http://www.oas.org/cyber/documents_en.asp

President's Commission on critical Infraestructure. (2012). Factsheet.*24th Air Force Home page*.Disponible en: http://www.24af.af.mil/library/factsheets/factsheet.asp?id=15663

Morris, R. (2012). *Universidad Politécnica de Madrid.*Disponible en: http://www.eui.upm.es/museo_virtual/4g/rtmorris

Senate Committee On Armed Services. (2014). AdmiralHaneyTestimony. Disponible en: https://archive.org/details/pdfy-oJoEPt1k8ej1oLCT

Stewart, W. (2014).Boot and program, viruses.Disponible en: http://www.livinginternet.com/i/is_vir_prog.htm

The Whitehouse.(1998). Presidential Decision Directive/nsc-63, 1998.Disponible en: www.whitehouse.gov/sites/default/files/omb/memoranda/.../m-04-15.pdf

The Whitehouse.(2011). State of the Union Speech 2011.Disponible en: http://www.whitehouse.gov/the-press-office/2011/01/25/remarks-president-state-union-address

The Whitehouse.(2012). State of the Union Speech 2012.Disponible en: http://www.whitehouse.gov/the-press-office/2012/01/24/remarks-president-state-union-address

The Whitehouse.(2013). State of the Union Speech 2013.Disponible en: http://www.whitehouse.gov/the-press-office/2013/02/12/president-barack-obamas-state-union-address

United States Senate. (2002). Testimony: Alan Paller. Disponible en: www.sans.org/press/

Van Munster.(2014). Securitization. *Oxford Bibliographies*. Disponible en: http://www.oxfordbibliographies.com/view/document/obo-9780199743292/obo-9780199743292-0091.xml