EL INDIVIDUO COMO INSTRUMENTO EN LA NARRATIVA DE CIBERSEGURIDAD INTERNACIONAL CONTEMPORÁNEA

PONTIFICIA UNIVERSIDAD JAVERIANA

FACULTAD DE CIENCIAS POLÍTICAS Y RELACIONES INTERNACIONALES

CARRERA DE RELACIONES INTERNACIONALES

BOGOTÁ D.C.

2019

EL INDIVIDUO COMO INSTRUMENTO EN LA NARRATIVA DE CIBERSEGURIDAD INTERNACIONAL CONTEMPORÁNEA

ALEJANDRA PABÓN BERMÚDEZ

PONTIFICIA UNIVERSIDAD JAVERIANA

FACULTAD DE CIENCIAS POLÍTICAS Y RELACIONES INTERNACIONALES

CARRERA DE RELACIONES INTERNACIONALES

BOGOTÁ D.C.

2019

TABLA DE CONTENIDO

1. INTRODUCCIÓN

"Mi único motivo es informar al público sobre lo que se hace en su nombre y lo que se hace contra ellos".

Edward Snowden

El ciberespacio, definido como un escenario donde se desenvuelve la serie de dinámicas relativas a la información y comunicación, presenta a los Estados una especie de paradoja: es por un lado una gran oportunidad y por otro, una significativa amenaza. De tal manera que se ha convertido en una prioridad para los Estados lograr establecer su narrativa de ciberseguridad como la dominante en el sistema internacional, demostrando una mayor capacidad e influencia que sus competidores.

En los últimos años la inseguridad que genera el ciberespacio tanto para los individuos como los Estados es de preocupación. Los Estados intentan dar respuestas a esta situación, pero estas en vez de ser prácticas generalmente vienen formuladas en un discurso. Esta investigación pretende analizar dichos discursos. Para tal fin se entenderán estos discursos como narrativas de securitización. Para comprender este término es menester definir sus partes: narrativa y securitización.

Se entiende una narrativa como un sistema de argumentaciones que crea una descripción de la realidad; de acuerdo con la semiología, el discurso narrativo desempeña un papel importante en los procesos de razonamiento y a menudo se emplea como herramienta de persuasión política para generar cohesión grupal.

> Las narrativas tienen un papel clave en la construcción social de la realidad, al dotarla de cierta racionalidad y coherencia, y evitar que se presente de manera ininteligible. Se configuran como marco interpretativo capaz de dotar de sentido a los hechos… Los discursos o narrativas definen expectativas, jerarquizan actores, asignan roles y funciones, prescriben comportamientos y una norma social respecto a la conducta aceptable o punible, estableciendo de antemano incentivos y penalizaciones. Tienen también un importante papel constitutivo de los intereses, valores e identidades de los actores políticos, y de las prácticas sociales en política exterior y en otros ámbitos. (Barbé, 2013, p. 33)

Entonces, las narrativas se presentan de manera intangible y permiten dar un sentido de racionalidad a la realidad y el contexto en el que se encuentra el ser. El discurso narrativo desempeña un papel de gran relevancia en los procesos de razonamiento y se emplea normalmente como herramienta de persuasión política para la cohesión grupal. Un ejemplo de lo anterior es el denominado *storytelling*, un mecanismo de propaganda electoral en el cual las narraciones y metáforas sustituyen los argumentos abstractos y los datos estadísticos, siendo más efectivos a nivel comunicativo para la movilización política o en el discurso nacionalista, esto es debido a que esta técnica vincula el pasado y el futuro (Barbé, 2013).

Por otro lado, el término securitización fue acuñado por Ole Weaver (el mayor representante de la Escuela de Copenhague) en 1995 como una reacción a los estudios tradicionales de seguridad, a las teorías realistas y neorrealistas que restringen el concepto de "amenaza" únicamente a peligros de tipo militar.

> Para Wæver, y otros como Barry Buzan, no era suficiente con analizar una amenaza militar, por ejemplo, aparentemente objetiva. Para estos autores lo importante era el estudio de: a) el proceso a través del cual ciertos actores, como la prensa o el Poder Ejecutivo, presentan ante el público la existencia de supuestas amenazas (militares o no militares) como un pretexto para desplegar ciertas medidas de emergencia; y b) los resultados de dicho proceso: por ejemplo, un incremento en el número de policías, mayores recursos, más armamento. (Treviño, 2016, p.3)

Por su parte, Wæver (1995) afirma que está en desacuerdo con dos premisas importantes del enfoque tradicional: la primera es que la seguridad es una realidad anterior al lenguaje, es decir existe independientemente de si la concepción es objetiva o subjetiva, en tanto que se mide en términos de amenazas o miedos; y la segunda, que en cuanto más seguridad mejor.

Después de todo, a pesar de todos los cambios de los últimos años, la seguridad, como con cualquier otro concepto, conlleva una historia y un conjunto de connotaciones de las que no puede escapar. En el corazón del concepto todavía encontramos algo que ver con la defensa y el Estado. "Como resultado, abordar un problema en términos de seguridad aún evoca una imagen de defensa de amenazas, asignando al estado un papel importante para resolverlo. Esto no siempre es una mejora" (Wæver, 1995, p. 46).

El autor expone el movimiento de la década de 1980 en el cual se amplía la agenda de la seguridad nacional hacia un enfoque holístico, enfatizando en la seguridad de las personas, ya sea como individuo o como colectividad global. Le seguridad del individuo se puede ver afectada de diversas maneras por fuera de los asuntos militares, como lo es la economía, la identidad, la cultura, etc.; es por esto por lo que se complica trazar un límite de lo aplicable en el enfoque holístico de seguridad, debido a que el concepto de seguridad se convierte en sinónimo de todo lo que es políticamente bueno o deseable. Para trazar dicho límite, Waever (1995) expone los textos de Johan Galtung y Jan Øberg, quienes formulan un concepto alternativo de seguridad, basado en cuatro conjuntos de objetivos positivos relacionados con las necesidades humanas: supervivencia, desarrollo, libertad e identidad, dando como resultado un programa holístico para la sociedad mundial. Dicho enfoque holístico parece ser algo positivo, pero contiene varias problemáticas. En primer lugar, el concepto de seguridad se torna demasiado amplio y todo puede ser incluido, transformándose en un concepto sin contenido; en segundo lugar, se causa una ausencia de efecto político en la “seguridad” como se define tradicionalmente.

El problema es que, como conceptos, no existe seguridad individual ni seguridad internacional. La seguridad nacional, es decir, la seguridad del Estado es el nombre de un debate en curso, una tradición, un conjunto establecido de prácticas y, como tal, el concepto tiene un referente bastante formalizado; a la inversa, evidentemente la "seguridad" de quien sea / lo que sea es una idea poco clara (Wæver, 1995).

Entonces a la pregunta ¿qué es lo que realmente hace que algo sea un problema de seguridad? Weaver (1995) responde:

> [Que] objetivamente los problemas de seguridad deberían ser catalogados como tal cuando son amenazas a la soberanía o independencia de un Estado de una manera particularmente rápida o dramática, y la privan de la capacidad de administrar por sí mismos. Sin embargo, operativamente, lo que realmente hace que algo sea catalogado como un problema de seguridad son las elites.
>
> Al nombrar un desarrollo determinado como un problema de seguridad, el "Estado" puede reclamar un derecho especial, uno que, en última instancia, siempre será definido por el estado y sus élites. (…) Por definición, algo es un problema de seguridad cuando las élites lo

> declaran así, por lo tanto, aquellos que administran esta orden pueden usarla fácilmente para propósitos específicos y de autoservicio es algo que no se puede ayudar fácilmente. (p.47)

A partir de esta definición de la seguridad Wæver (1995) afirma que se puede considerar la "seguridad" como un acto de habla. Según él "en este uso, la seguridad no es de interés como un signo que se refiere a algo más real; la expresión misma es el acto. Al decirlo, se hace algo (como apostar o prometer)" (p.48).

Teniendo una mejor comprensión de las narrativas de securitización, prosígase a exponer que estas, normalmente, están integradas en un orden internacional. Sin embargo, el orden internacional en materia del ciberespacio no se ha conformado. Esta investigación entonces plantea la pregunta ¿se instrumentaliza al individuo en las narrativas de ciberseguridad?

Entonces, el objetivo principal de esta investigación es determinar si hay una instrumentalización del individuo por parte de los gobiernos en las narrativas de ciberseguridad. En ese orden de ideas, los objetivos específicos de la investigación se organizan de la siguiente manera:

1) Exponer la problemática internacional causada por la falta de consenso frente al ciberespacio y su normatividad.
2) Analizar las tres narrativas predominantes contemporáneas, identificando su discurso, así como las similitudes y diferencias entre estas.
3) Exponer la evolución de la narrativa de Estados Unidos sobre la ciberseguridad como caso de estudio, a través del análisis histórico y de discurso.
4) Exponer las implicaciones de la narrativa contemporánea de Estados Unidos de ciberseguridad para el individuo y las libertades individuales.

La importancia y justificación de esta investigación reside en el hecho de que el uso de la TIC (Tecnologías de Información y Comunicación) por parte de gobiernos y empresas privadas, ha sido un medio a través del cual en ocasiones se vulnera el derecho de intimidad/privacidad de los individuos.

El derecho a la privacidad o intimidad ha sido reconocido desde el siglo XIX, se destaca entra los derechos fundamentales a la personalidad y se reconoció con anterioridad a los derechos sociales, por lo cual se podría ubicar en la primera generación de los DDHH. Este

derecho sirvió como base para la creación de mecanismos de protección de los datos personales.

Como se puede apreciar, el derecho a la privacidad es de gran importancia, y es por esto que la presente investigación busca evidenciar cómo se está vulnerando este derecho actualmente por parte de los gobiernos, con el fin de obtener información valiosa y utilizable para mejorar sus capacidades en el ciberespacio. Estados Unidos particularmente debido a su capacidad como creador de normas y a su rol en la creación y desarrollo de internet ha sido capaz de posicionar su narrativa como la preponderante en el sistema internacional, por esto es necesario analizar dicha narrativa y el lugar del individuo en esta. Es claro que el ciberespacio representa un desafío para el sistema internacional y las teorías tradicionales de seguridad, siendo muy compleja la adaptación de su administración a formas tradicionales de organización internacional. Este es un problema que se debe abordar de manera urgente para el mantenimiento de la paz y la seguridad en el mundo. Sin embargo, no se debe justificar las medidas de "seguridad" con derechos como la libertad y privacidad de las personas, en especial cuando estos están siendo vulnerados.

El problema de fondo consiste en que, al no existir un consenso internacional sobre el derecho y la soberanía en el ciberespacio, se genera una competencia de capacidades entre los países. Esta tiene el fin de agotar los recursos de los Estados, forzándolos a una negociación para escoger un Estado o ente regulador, siendo este el país que más capacidades posea para imponer su narrativa en el derecho internacional. Debido a esta competencia los Estados generan constantemente amenazas y ataques de ciberseguridad con el fin de que el individuo se vea afectado y vulnerable, lo cual lo llevará a ceder su privacidad y libertades individuales a cambio de una mayor securitización.

Para realizar un análisis de esta problemática, existen ciertos recursos y limitantes a saber. Los métodos que se utilizaron en la investigación fueron cualitativos y se denominan: *process traicing*, representación histórica, y el análisis de discurso. Estos tres métodos se emplearon a lo largo de la investigación para finalmente, a partir del análisis realizado, llegar a inferir la mejor explicación causal a la securitización del ciberespacio y la instrumentalización del individuo. A lo anterior se le denomina "inferencia a la mejor explicación" y se encuentra

dentro de la epistemología del realismo crítico. A continuación, se realiza una breve explicación de los métodos mencionados anteriormente.

a) Process traicing

En la utilización de este método se debe procurar no perder de vista el panorama general, ser conscientes de los requisitos de datos significativos del método y reconocer los supuestos epistemológicos inherentes a su aplicación. Primero se deben comprender ciertos conceptos básicos de un enfoque basado en procesos y mecanismos para el estudio de la política internacional.

Además, se debe tener en cuenta el concepto del mecanismo como un conjunto de hipótesis que podría ser la explicación de algún fenómeno social. Este mecanismo opera a un nivel analítico dentro de una teoría más amplia y aumenta la credibilidad de la teoría al dar explicaciones más detalladas. Los mecanismos entonces conectan unas condiciones iniciales con el resultado en una situación específica. Por ejemplo, en un proyecto en que se busca solucionar algún problema social, entonces se debe buscar una causa A y una solución que genere un efecto B, para este fin se teorizan diferentes mecanismos sociales que pueden ser genéricos (cálculo estratégico, juego de roles y persuasión normativa) que permitan plantear conexiones entre A y B.

> Metodológicamente, el rastreo de procesos proporciona información práctica sobre cómo llegar a conocer las tuercas y los pernos para las cuentas de cambio social basadas en mecanismos. Pero también lo dirige a uno para rastrear el proceso de una manera muy específica, teóricamente informada. (Prakash y Klotz, 2008, p.116)

Al abordar el tema de los mecanismos y el rastreo de procesos se puede hablar de un nivel micro y un nivel macro. El nivel micro seria lo que se denomina mecanismo de agente a agente, el cual examina dinámicas de toma de decisiones específicas. El nivel macro se enfoca en el estudio de los mecanismos causales, es decir, causales en términos lineales. En resumen, “el proceso de rastreo significa rastrear la operación de los mecanismos causales que funcionan en una situación dada. Uno mapea cuidadosamente el proceso, explorando hasta qué punto coincide con las expectativas previas, teóricamente derivadas, sobre el funcionamiento del mecanismo” (Prakash y Klotz, 2008, p.116).

Así pues, los datos para el rastreo de procesos son de naturaleza cualitativa (entrevistas, documentos, informes de prensa, etc.). El proceso de rastreo se puede utilizar en cuestiones de interacciones agente-agente y en el establecimiento de contexto estructural en una situación o periodo temporal dado. El desafío mayor es la cantidad de tiempo y datos que requiere el análisis.

En la presente investigación el rastreo de procesos se hizo con un enfoque macro, buscando como objetivo establecer el contexto estructural del proceso de desarrollo de la narrativa internacional de ciberseguridad de Estados Unidos.

b) Representaciones históricas

Las autoras Prakash y Klotz (2008) afirman que la "realidad" es incognoscible fuera de la percepción humana y no hay una autoridad absoluta en un tema dado, es por esto que se puede afirmar que las sociedades construyen representaciones.

> Por representación histórica, me refiero a cómo se ha representado el objeto de una consulta (X) en el tiempo y el espacio. X puede ser cualquier cosa: un país (el Congo), una nación o comunidad (los kurdos), una persona (Saddam Hussein) o un concepto (soberanía)... Las sociedades producen, circulan y consumen discursivamente representaciones de X, construyendo lo que a menudo se denomina "regímenes de verdad" o "conocimiento". (Prakash y Klotz , 2008, p.79)

Estos denominados "regímenes de verdad" se convierten en discursos que componen secuencias significativas, y estas a su vez, constituyen marcos coherentes de las acciones y declaraciones. Entonces, a diferencia de otros, este enfoque discursivo de las relaciones internacionales rechaza la idea que los recursos pueden explicarse fuera de su contexto discursivo; se debe comprender entonces que la interacción social está influenciada por clasificaciones, guiones cognitivos y racionalidades.

Entonces, tenemos unas representaciones de la realidad y sus secuencias dentro de los discursos, estos elementos permiten analizar el poder y comprender que este es un sistema socialmente construido a partir de la práctica del conocimiento. Sin embargo, es de gran importancia el hecho de que la identidad, los significados y características están vinculados

al contexto en el cual se construyen; las prácticas de nomenclatura podrían significar algo diferente para las personas que viven en diferentes culturas o épocas.

Las representaciones, aunque son invenciones basadas en el lenguaje tienen implicaciones políticas evidentes debido a que permiten a los actores conocer y actuar sobre un objeto dado. Es importante comprender cómo ciertas estructuras de conocimiento se vuelven dominantes; los significados e identidades aceptados en el común llegan a tal estado de aceptación debido a la fuerza de esa representación específica.

> La producción y la circulación de discursos son políticamente controvertidos, y el discurso que ganará aceptación social dependerá en gran parte de la distribución del poder… Uno puede investigar el funcionamiento del poder en la producción de discursos explorando la lucha sobre quién puede hablar con autoridad. (Prakash y Klotz, 2008, p.81)

Por lo tanto, el poder también se ejerce a través del proceso de circulación, debido a que los discursos están en constante competencia por tener mayor aceptación y reproducción social; este es el caso de los diferentes discursos de la ciberseguridad. Diferentes factores y razones llevan a que un discurso gane hegemonía; "el poder, como los discursos, nunca está totalmente centralizado. Un objetivo principal de este enfoque es explorar la relación entre el discurso y el poder en relación con la representación" (Prakash y Klotz, 2008, p.81).

Para lograr el análisis de las representaciones históricas en la presente investigación se tiene en cuenta la multiplicidad y controversia de los discursos; las formas diferentes en que el poder funciona a través de procesos de producción y circulación y el reconocimiento de la subjetividad del investigador. Para este enfoque, además, la agencia de las personas y sus acciones se dan debido a la comprensión discursiva que estas tengan del mundo y su lugar en él, y no por intereses universales, preferencias de medios y fines, o incluso normas y valores internalizados, como se asume generalmente.

Finalmente, se debe reconocer que la investigadora del presente escrito posee un sesgo que surge de su contexto social. "Permítanme simplemente señalar que creo que los historiadores producen sus propios "regímenes de verdad," no objetiva. La historia produce su propia discursos. La investigación es altamente discutida, y el historiador no es neutral" (Prakash y Klotz, 2008, p.81).

c) Análisis de Discurso

El método del análisis de discurso expone el hecho de que las representaciones que se repiten constantemente se convierten en un conjunto de declaraciones y prácticas, a través de las cuales el lenguaje se institucionaliza y por lo tanto se normaliza; se deben tener en cuenta factores como el nivel de influencia de dichas representaciones. “Cuando las personas que expresan las mismas representaciones se organizan, se posicionan en el discurso” (Prakash y Klotz, 2008, p.61).

Al igual que las representaciones, las posiciones de los discursos pueden ser dominantes o marginados en varios grados. Por ejemplo, se puede demostrar que un discurso está institucionalizado si se evidencia que las metáforas aparecen regularmente en los mismos textos. “Cuanto más se puedan especificar empíricamente tales cosas, mejor será el análisis. Lo ideal es incluir tantas representaciones y sus variaciones como sea posible, y especificar dónde se encuentran en el mayor grado posible” (Prakash y Klotz, 2008, p.62).

Estas investigadoras expusieron lo anterior poniendo como ejemplo sus descubrimientos sobre el análisis del discurso europeo sobre Rusia, en el cual encontraron “una representación que enfatizaba que las mujeres rusas habían sido violadas por los hombres mongoles y tártaros durante siglos, y que esto había fomentado a un pueblo particularmente salvaje y bárbaro” (Prakash y Klotz, 2008, p.62). Según las autoras esta representación se formó muchos años atrás, logró una popularidad en el periodo entre guerras y luego se sumergió en el discurso europeo. En los Estados bálticos, esta representación tuvo gran influencia en el periodo soviético y los años noventa.

> La primera tarea de investigación es mostrar las afinidades y diferencias entre las representaciones para demostrar si pertenecen al mismo discurso. Pero la repetición no excluye la variación o la representación gradual, por lo que el análisis del discurso también busca captar los inevitables cambios culturales en las representaciones de la realidad. (Prakash y Klotz, 2008, p.62)

El análisis de discurso es de gran utilidad para comprender la regularidad en las relaciones sociales, porque este produce condiciones previas para la acción y limita cómo se ordenan los elementos de los cuales se compone el mundo, y, por lo tanto, cómo se clasifican las

personas según su manera de pensar sobre el mundo. El discurso limita las acciones que se consideran posibles o normales en el contexto dado. “Pero el discurso no puede determinar la acción por completo. Siempre habrá más de un resultado posible. El análisis del discurso tiene como objetivo especificar el ancho de banda de los posibles resultados” (Prakash y Klotz, 2008, p.62).

Para concluir esta introducción prosígase a exponer la estructura de la presente investigación, la cual se organiza de la siguiente manera: en el primer capítulo, se analizan las tres narrativas predominantes sobre la ciberseguridad, de la manera que se presentan contemporáneamente, para identificar diferencias y similitudes entre ellas, así como los bloques de países que las respaldan. Posteriormente en el segundo capítulo se realiza un estudio de caso utilizando el análisis histórico enfocado en la narrativa de Estados Unidos.

Dicha narrativa, la cual afirma que el ciberespacio es un campo que los Estados tienen vocación a regular, y cuya la regulación se debe lograr mediante el derecho internacional, ha sido la preponderante en el sistema internacional, pero ha sufrido varios cambios a lo largo de la historia debido a diferentes contextos e hitos históricos relevantes para comprender la securitización del ciberespacio.

2. MARCO TEORICO

El objetivo de esta investigación es determinar si se instrumentaliza al individuo en las narrativas de ciberseguridad. Para lograr este objetivo es necesario analizar el proceso de construcción de los discursos y narrativas de los Estados en el ámbito de la ciberseguridad internacional. Con este fin se deben comprender diferentes conceptos enmarcados respectivamente en una corriente teórica.

Esta investigación contiene ciertos limitantes conceptuales y teóricos que se deben exponer en aras de comprender los conceptos a saber y las bases teóricas de la investigación. Entonces, siendo que la finalidad es lograr evidenciar la narrativa discursiva de los Estados y sus acciones, el realismo y el liberalismo (aunque permiten comprender los conceptos y

limitaciones de la investigación) no permiten analizar el proceso de construcción de dichas narrativas y discursos; es por esto que la Escuela Inglesa, específicamente el enfoque de la securitización dentro de esta (al cual se le denomina Escuela de Copenhague) será la teoría base para responder la pregunta, dado que esta contiene elementos del realismo y liberalismo pero también tiene influencias de la teoría constructivista.

Siendo que el objeto de estudio son las narrativas de los Estados, se acepta que el Estado es el actor principal en las relaciones internacionales, es por esto que dicho concepto se define a partir de la teoría realista, apoyada en los principales autores de esta. Se acepta además que el ciberespacio es un ámbito anárquico, debido a la falta de consenso en cuanto a las normas internacionales a aplicar en dicho espacio, por lo que el concepto de la anarquía también lo basaré en la teoría realista. Sin embargo, se asume que las normas permiten modificar el comportamiento de los Estados, es por esto por lo que se debe analizar el concepto de la normatividad desde la teoría liberal de las relaciones internacionales; entre estas normas, para fines de la investigación, se le da prioridad a la norma de la privacidad.

2.1 Estado

El Estado en la teoría realista se entiende como el actor central de las relaciones internacionales. El modelo de Morgenthau es estatocéntrico, debido a que afirma que el Estado es el actor por excelencia en el sistema internacional contemporáneo, siendo este un actor racional, con un interés nacional. (Barbé, 1987) Este concepto estatocéntrico, para Morgenthau, se sitúa en dos categorías de análisis: el interés nacional y el equilibrio de poder.

El equilibrio de poder Morgenthau lo describe como la configuración que surge a partir de las acciones de las naciones impulsadas por el deseo de poder, que llevan a la configuración del status quo, este es el denominado equilibro de poder (Barbé, 1987).

El segundo elemento, el interés nacional, se refiere a la prioridad de la existencia y supervivencia del Estado-Nación, un fenómeno explicado también por Morgenthau; cuyas obras se convirtieron en las bases de la teoría realista (Barbé, 1987).

Es importante comprender que dicha teoría surge en el contexto de la Segunda Guerra Mundial, por lo tanto, contiene postulados de defensa del Estado como actor central del

sistema internacional y del medio de la fuerza para disuadir a demás actores internacionales. Entonces, se puede afirmar que esta teoría intenta comprender los sucesos en el sistema internacional a partir de la disputa de poder (Muñoz & Frasson, 2011).

Otro elemento importante de esta definición estatocentrista del realismo para la investigación es la visión de la naturaleza humana. Los postulados de Morgenthau subrayan la importancia de las ideas de Hobbes, quien afirma que la naturaleza del humano es conflictiva y egoísta, esto ocasiona las guerras y conflictos en general. Hobbes además analiza cómo el humano puede sobre pasar su naturaleza a través de la creación de una autoridad y normatividad que regule el comportamiento en sociedad. Para el realismo clásico, la seguridad y la supervivencia del Estado son los dos elementos esenciales para la supremacía del Estado. El poder militar y el derecho internacional se consideran herramientas para asegurar dicha seguridad y supervivencia. Esta postura afirma además que la ley internacional será acoplada siempre y cuando no debilite al Estado, de lo contrario puede ser ignorada (Muñoz & Frasson, 2011).

El realismo clásico y sus pensadores fueron una base poderosa para el desarrollo de la corriente; en el siglo XX se construyen los aportes principales a la corriente, en el contexto de la post guerra fría, debido a factores como el fallido modelo de orden mundial diseñado por Woodrow Wilson y la tensión internacional (Muñoz & Frasson, 2011).

En este orden de ideas, los postulados principales que se exponen de la teoría realista en el siglo XX son tres: primero, que existen unas reglas de juego basadas en los principios y acuerdos y estas pueden tener prioridad sobre las reglas; segundo, que las reglas e instituciones establecidas imponen límites en el ejercicio de poder. Finalmente, que las reglas e instituciones son estructuradas para el sistema y no solamente para unas partes (Muñoz & Frasson, 2011).

En conclusión, la teoría realista nos aporta a la investigación en cuanto apoya los siguientes postulados (Muñoz & Frasson, 2011):

- La unidad de análisis es el Estado, entendido como actor unitario y racional, lo cual se evidencia en su actuar en busca de la maximización de poder.

- La problemática de estudio es la seguridad nacional. Se desarrolla enfocada en la supervivencia del Estado en un medio hostil.
- -El sistema internacional, así como el ciberespacio, son anárquicos debido a la falta de consenso en la norma internacional.

2.2 Anarquía

Como se ha mencionado la anarquía es otro concepto que se asume en la teoría realista. En el modelo de Morgenthau, esta se basa en dos factores primarios: la multiplicidad de unidades y el antagonismo entre ellas (Barbé, 1987).

En su libro "Politics among nations" Morgenthau afirma que el carácter de las relaciones internacionales es anárquico, basado en la naturaleza conflictiva del ser humano, explicada en los postulados de Hobbes. Es por esto por lo que la conclusión de Morgenthau es que no puede existir un orden legal viable o una paz permanente en el sistema internacional. Entonces, el sistema internacional, siendo que se constituye centralmente de Estados soberanos, carece de un poder centralizado y es naturalmente conflictivo. Consecuentemente, el sistema de Estados es de carácter histórico y no permanente; sin embargo, el conflicto permanece en la concepción del propio sistema y de la política. Entonces todo acto político se realiza en busca de la maximización de poder y por lo tanto es inherente a la naturaleza anárquica y conflictiva (Barbé, 1987).

Tal como se ha dicho, el interés nacional se refiere a la supervivencia del Estado, entonces en orden de cumplir este objetivo los Estados buscan maximizar su poder, esto se comprende bajo el concepto de la "autoayuda", una doctrina basada en la motivación de supervivencia del Estado, lo cual asume que los Estados no pueden confiar en las alianzas o en demás actores y esto también es un factor importante para definir dicha anarquía. Pensadores como Maquiavelo, analizaban el deseo de poder que es inherente a la naturaleza humana y se extiende al ámbito político; a igual que Hobbes y Morgenthau, este afirma que la naturaleza conflictiva del hombre lleva a que la política sea una lucha de poder y capacidad (Barbé, 1987).

Aunque se debe hacer la salvedad que, la teoría realista define el poder y las capacidades principalmente en términos militares y no se enfoca en el poder de las narrativas y los discursos, es por esto por lo que más adelante se definirá el concepto de narrativa tomando como base diferentes teorías para comprender su aplicación en el sistema internacional contemporáneo.

2.3 Sistema Internacional

El sistema internacional es definido por la profesora Barbé (como se citó en Orozco, 2013) como "la configuración de poder generada por las potencias del sistema (…) Sus variables fundamentales son el número de actores y la distribución del poder entre ellos" (p. 217). Según lo anterior y observando el contexto de la configuración de poder en el mundo se puede inferir lo siguiente:

> Actualmente el sistema político internacional es semejante a una mesa de negociación en la que coexisten los diferentes actores estatales y no estatales con capacidad de ejercer poder para crear las reglas de juego y usarlas en su favor y en la que se vinculan a través de relaciones complejas de tensión/distensión y de división/complementariedad. (Orozco, 2013, p.108)

Entonces, en la época contemporánea el sistema internacional se entiende como un conjunto de dinámicas determinadas por un sistema de acuerdos y alianzas de los principales actores mundiales, los cuales utilizan herramientas de disuasión como la coerción o la influencia. Se debe hacer la salvedad de que, a pesar de que exista un sistema configurado por alianzas, esto no significa que el interés nacional de los Estados no incluye pretensiones de posicionarse como hegemónicos; por el contrario, la imposición o hegemonía global de un solo Estado o un grupo reducido de Estados es lo que permite que se construyan estas alianzas (Orozco, 2013).

Hoffman en su obra "A New World Order and Its Troubles" afirma que el mundo se encuentra en un sistema multicentrista en el cual las potencias ejercen como tales en su área específica: Rusia en el área militar, Japón y Alemania en el área económica-financiera, China e India en el área demográfica y Estados Unidos en el área económica-militar. A pesar de esto, al contrastar el poder de Estados Unidos en diferentes áreas la opinión mayoritaria

reconoce un sistema de unipolaridad estadounidense. De cualquier manera, todos los Estados están en constante búsqueda de aumentar sus capacidades y su posición e influencia en el sistema internacional y esto es lo que los lleva a securitizar diferentes temas de la agenda nacional; securitizar un ítem significa que este se vuelve un tema de importancia para la seguridad nacional, al adquirir dicha posición se le da más campo de acción a los dirigentes para tomar decisiones y realizar acciones frente al tema en cuestión (Orozco, 2013).

3. NARRATIVAS DE CIBERSEGURIDAD DOMINANTES

Para fines de la investigación se debe realizar una contextualización de las diferentes narrativas para poder contrastar sus diferencias y similitudes. De esta manera se evidenciarán las diferentes posturas frente a la privacidad y los derechos individuales en el ciberespacio. Se debe comprender además que cada país maneja una narrativa y un discurso internacional independiente de sus acciones y políticas nacionales. Finalmente, este capítulo presenta evidencia de la fuerte competencia entre las diferentes narrativas por ser la dominante en el sistema internacional, y las implicaciones que esto conlleva.

Con este fin se realiza un breve análisis de las tres narrativas dominantes en el siguiente orden: Estados Unidos, Rusia y China. Este análisis se centrará únicamente en el discurso y narrativa contemporáneos, exponiendo las posturas y acciones evidenciadas en cada país durante la administración actual.

3.1 Estados Unidos

La narrativa de Estados Unidos afirma que el ciberespacio es un espacio que los Estados tienen vocación a regular y que la capacidad de regular únicamente la tiene Estados Unidos. Afirma que esta regulación debe ser estipulada en una normatividad, la cual se debe crear mediante el derecho internacional y la cooperación bajo el liderazgo de Estados Unidos.

En ese sentido, el presidente Trump promulgó la Ley de la Ciberseguridad y La Agencia de Infraestructura de seguridad en noviembre de 2018, lo cual sentó las bases de la Estrategia de Ciberseguridad Nacional (a la cual nos referiremos cómo La Estrategia de ahora en adelante) también aprobada en noviembre de 2018 (White House, 2018).

La Estrategia plantea de manera concisa la importancia del ciberespacio en la agenda de seguridad nacional, expone la definición del término, se refiere a amenazas conclusas y señala países concretos como competencia directa. En todo el documento se expone una posición "salvadora" por parte de Estados Unidos, y presenta a los países competidores como obstáculos ilegítimos a la construcción de un orden internacional benevolente, Además, el documento presenta estrategias y acciones concretas a realizar para lograr el objetivo de la visión estadounidense, que afirman es "asegurar una Internet abierta, interoperable, confiable y segura" y afirma que estas acciones se realizaran de una manera ofensiva. A continuación, analizaremos la Estrategia de manera detallada" (White House, 2018, p. 8).

El documento se introduce con un fragmento escrito por el presidente Trump. En este él afirma que "América creó Internet y la compartió con el mundo. Ahora, debemos asegurarnos de proteger y preservar el ciberespacio para las generaciones futuras". En este discurso se observa la posición de Estados Unidos, en la cual se autoproclama líder en la gobernanza del ciberespacio y el único capaz de crear una normatividad para este. Más adelante esta posición se reafirma y se complementa exponiendo las supuestas intenciones del país:

> El ciberespacio es un componente inseparable de la vida financiera, social, gubernamental y política de los Estados Unidos. Mientras tanto, los estadounidenses daban por sentado que la supremacía de los Estados Unidos en el dominio cibernético no sería cuestionada (…) Los estadounidenses creían que el crecimiento de Internet fomentaría las aspiraciones universales de libertad de expresión y libertad individual en todo el mundo. Además, asumieron que las oportunidades para expandir la comunicación, el comercio y el libre intercambio de ideas serían evidentes. (White House, 2018, p.1)

Prosigue con la exposición de su posición internacional frente a las demás narrativas, al afirmar que estas no solo son erróneas, sino que son nocivas y deben ser eliminadas, y que Estados Unidos es el único país capaz de proveer una gobernanza efectiva para el ciberespacio, debido a sus ideales. En esta parte del documento se refieren a países y amenazas en concreto. Señalando de una manera directa cualquier pensamiento diferente al de Estados Unidos y reconociendo la existencia de una competencia constante entre narrativas estatales.

En el texto se expone que, aunque muchos países apoyan la visión de Estados Unidos de un ciberespacio abierto y compartido, los competidores y adversarios del país han adoptado una posición opuesta. Estos países opositores "se benefician de la Internet abierta, al tiempo que restringen y controlan el acceso de su propia gente, y socavan los principios de una Internet abierta en los foros internacionales", y, además, utilizan la soberanía como excusa para violar las leyes de otros estados al participar en actividades de espionaje económico y político. En el documento se asevera lo que sigue:

> La Administración reconoce que los Estados Unidos participan en una competencia continua contra adversarios estratégicos, estados deshonestos y redes terroristas y criminales. Rusia, China, Irán y Corea del Norte utilizan el ciberespacio como un medio para desafiar a los Estados Unidos, sus aliados y socios, a menudo con una imprudencia que nunca considerarían en otros dominios. Estos adversarios utilizan herramientas cibernéticas para socavar nuestra economía y democracia, robar nuestra propiedad intelectual y sembrar la discordia en nuestros procesos democráticos. Somos vulnerables a los ataques cibernéticos en tiempos de paz contra infraestructuras críticas, y aumenta el riesgo de que estos países realicen ataques cibernéticos contra Estados Unidos durante una crisis sin guerra. Estos adversarios están continuamente desarrollando nuevas y más efectivas armas cibernéticas. (White House, 2018, p.1)

Posteriormente, se exponen y desarrollan los cuatro pilares de la Estrategia, es decir el cómo se logrará lo expuesto anteriormente. Estos pilares se denominan y explican brevemente de la siguiente manera (White House, 2018):

I. Proteger al pueblo estadounidense a la patria y al estilo de vida estadounidense. A través de la protección de redes, sistemas, funciones y datos.
II. Promover la prosperidad estadounidense. A través del fomento de la innovación nacional y el manejo de una economía digital segura y prospera.
III. Preservar la paz y seguridad a través de la fuerza. El fortalecimiento de la capacidad de los Estados Unidos, en concierto con aliados y socios, para disuadir y, si es necesario, castigar a quienes usan herramientas cibernéticas con fines maliciosos.
IV. Expansión de la influencia estadounidense en el extranjero. Esto con el fin de extender los principios clave de una Internet abierta, interoperable, confiable y segura.

Considerando que el interés de la investigación reside en el discurso y la narrativa de Estados Unidos en esta investigación no se aborda de manera detallada las acciones descritas para cada pilar. Sin embargo, sí se examina el texto en dos pilares importantes.

Primero el pilar denominado "Preservar la paz y seguridad a través de la fuerza". El título y el contenido de este fragmento del documento permite evidenciar, primero que para Estados Unidos el ciberespacio no solo es un tema de seguridad, sino que el país ha tomado una posición ofensiva frente al tema y está decidido a erradicar cualquier amenaza y tomar cualquier medida contra sus competidores; y segundo, que esta posición de imposición de normas a través de la fuerza, el gobierno la justifica con "la preservación de la paz y la seguridad".

> Los Estados Unidos utilizarán todas las herramientas apropiadas del poder nacional para exponer y contrarrestar la inundación de la influencia maligna en línea y las campañas de información y la propaganda y la desinformación no estatal. Esto incluye trabajar con socios de gobiernos extranjeros, así como con el sector privado, la academia y la sociedad civil para identificar, contrarrestar y prevenir el uso de plataformas digitales para operaciones de influencia extranjera maligna, respetando los derechos civiles y las libertades…Todos los instrumentos del poder nacional están disponibles para prevenir, responder y disuadir la actividad cibernética malintencionada contra los Estados Unidos. Esto incluye capacidades diplomáticas, de información, militares (tanto cinéticas como cibernéticas), financieras, de inteligencia, de atribución pública y de aplicación de la ley. (White House, 2018, p. 21)

Esta posición se puede evidenciar a través de las sanciones y demás medidas tomadas por parte de Estados Unidos en contra de los países opositores a su ideología. Un ejemplo de esto son las sanciones aplicadas a Rusia en 2018. Estados Unidos sancionó varias compañías y a tres individuos rusos bajo la acusación de colaborar con la principal agencia de inteligencia de dicho país. Las entidades e individuos sancionados tienen prohibido ser partícipes de cualquier transacción que involucre el sistema financiero de los Estados Unidos (Rennack & Welt, 2019).

Un segundo ejemplo se encuentra en las sanciones impuestas por Estados Unidos hacía Irán en 2018. La administración de Trump utilizó la Orden Ejecutiva 13694 para sancionar a las entidades iraníes determinadas a participar en actividades cibernéticas maliciosas o en

delitos transnacionales. La Orden Ejecutiva 13694 bloquea la propiedad basada en los Estados Unidos de entidades extranjeras que se determinó que han participado en actividades cibernéticas que (1) perjudican o comprometen la provisión de servicios por parte de computadoras o redes de computadoras que brindan apoyo en el sector de infraestructura crítica; (2) comprometen infraestructura crítica; (3) interrumpen las computadoras o las redes de computadoras; o (4) causan la malversación de fondos, secretos comerciales, identificadores personales o información financiera para obtener una ventaja o ganancia financiera (Katzman, 2019).

Complementando lo anterior, se analiza un segundo pilar, el denominado "Expansión de la influencia estadounidense en el extranjero", este es de gran importancia porque evidencia el interés de aumentar el poder de Estados Unidos en el ciberespacio y la instrumentalización del individuo para lograr este fin, dado que en el texto se afirma lo siguiente:

> El gobierno de los Estados Unidos conceptualiza la libertad en Internet como el ejercicio en línea de los derechos humanos y las libertades fundamentales, como las libertades de expresión, asociación, reunión pacífica, religión o creencia *y derechos de privacidad en línea*, independientemente de las fronteras o el medio. Por extensión, la libertad de Internet también apoya el libre flujo de información en línea que mejora el comercio internacional, fomenta la innovación y fortalece la seguridad nacional e internacional. Como tal, los principios de libertad de Internet de Estados Unidos están inextricablemente vinculados a nuestra seguridad nacional. (…) Dada su importancia, los Estados Unidos alentarán a otros países a promover la libertad en Internet a través de lugares como la Coalición en línea de la Libertad, de la que Estados Unidos es miembro fundador. (White House, 2018, p.24, cursiva añadida)

Así pues, es posible apreciar por el nombre y la descripción de este pilar que la intención de Estados Unidos es consolidar y fortalecer su red de aliados, públicos, privados y de la sociedad civil entera, tanto de productores de conocimiento como usuarios. Esto para generar un bloque ideológico de países que apoyen su posición y extiendan su influencia. Este fin lo han logrado a través de su influencia en organizaciones como la ONU. Es por esto que Estados Unidos es capaz de ejercer mayor presión, y castigos más severos, a los países que atenten contra su discurso o se opongan a este. Sin embargo, Rusia y China también han

consolidado un bloque de países que apoyan su posición frente al ciberespacio, aunque su influencia en organizaciones internacionales no es tan grande como la de Estados Unidos.

Se debe mencionar además que existe una propuesta estadounidense paralela de regulación del ciberespacio. La cual plantea que la regulación sea igual que en los intercambios financieros normales en donde funcionaría un principio de extraterritorialidad del derecho estadounidense. Sin embargo, esta propuesta no tiene tanto apoyo como el discurso que Estados Unidos ha construido en donde se presenta como mesías, salvador de los derechos y libertades.

Entonces, para concluir, se puede afirmar que la narrativa de securitización del ciberespacio de Estados Unidos expone que este es un espacio que debe ser regulado, pero que el referido país es el único idóneo para liderar el proceso de creación de normas internacionales para el ciberespacio. Esta posición la justifica a través del argumento de que los Estados Unidos es el país que defiende los ideales de la paz y la seguridad para los individuos y por esto los demás países deben seguir su liderazgo. Entonces, las libertades individuales y la privacidad son centrales en el discurso y la narrativa de Estados Unidos, a pesar de que esto no se refleje en sus acciones.

3.2 Rusia

La narrativa interna de ciberseguridad rusa comparte ciertos lineamientos con la narrativa de EE. UU en cuanto se basa en la idea de protección de datos y libertades, esto se puede evidenciar en la ley de protección de datos o ley de privacidad de 2006. Mientras que la narrativa internacional rusa sobre ciberseguridad difiere completamente de la de EE. UU; ya que, en vez de considerar un regulador, afirma que el ciberespacio debe ser anárquico, de manera que cada Estado debe asumir las acciones de defensa y ataque de su ciberespacio con sus capacidades y según su criterio.

Estas narrativas de Rusia se pueden evidenciar a través de diferentes ejemplos. Para comenzar se tiene en cuenta el discurso presentado por el presidente ruso Vladimir Putin durante la sesión plenaria del Congreso Internacional de Ciberseguridad organizado por Sberbank, Data Economy y la Asociación de Bancos de Rusia, el cual se llevó a cabo en

Moscú, los días 5 y 6 de julio del año 2018 y contó con la asistencia de los jefes de las principales empresas rusas y extranjeras, proveedores de software y servicios de ciberseguridad, funcionarios federales rusos y expertos mundiales.

En primer lugar, el presidente reafirma la importancia del uso de la tecnología en la actualidad y la necesidad de implementarla en todas las áreas posibles para facilitar el manejo de la información, el crecimiento económico, y la eficiencia de las actividades de agencias gubernamentales y privadas. La primera parte de su discurso expone la narrativa interna sobre la ciberseguridad, afirmando que dentro del país se están realizando grandes avances y esfuerzos por ganar un mejor nivel de digitalización, y que esto se hace con el fin de mejorar el bienestar de las personas; además señala de manera explícita la importancia que tiene para el gobierno ruso el respeto de los derechos y libertades en el manejo del ciberespacio a nivel nacional. Putin afirmó:

> Entendemos que la digitalización es un motor crucial del desarrollo nacional y puede realmente mejorar el bienestar de las personas … Al mismo tiempo, me gustaría señalar que el desarrollo digital efectivo solo puede basarse en una libertad digital para las empresas, las organizaciones públicas, los ciudadanos, para eliminar las barreras que dificultan el progreso. Pero, sin embargo, todos debemos entender la responsabilidad y los riesgos potenciales, las amenazas y los desafíos de la esfera digital. (Putin, 2018)

Continuando con la exposición del manejo de la ciberseguridad interna de Rusia, el presidente afirma que el país ocupa el primer lugar en Europa en términos de usuarios de internet y que el comercio online está creciendo de manera rápida; además, que los ciudadanos rusos actualmente gozan de servicios estatales y municipales cada vez más digitalizados, lo cual ahorra tiempo y esfuerzo para ambas partes. Sin embargo, esta digitalización viene con consecuencias y riesgos, es por esto que Rusia ha adoptado medidas como el programa de Economía Digital, el cual tiene como fin lograr una mejor eficiencia en la digitalización del área económica y social, y de administración pública.

> El programa da prioridad a la creación de regulaciones legales flexibles, que deben tener en cuenta los aspectos específicos de la industria, y no obstaculizar, sino seguir el avance del desarrollo de la tecnología digital. También debe proteger las libertades económicas, la propiedad, la seguridad, la vida privada y el espacio personal de los ciudadanos. (Putin, 2018)

Esto permite evidenciar que a nivel nacional Rusia ha avanzado de gran manera en el uso del ciberespacio para la mejora de la calidad de vida y que además hay una preocupación explícita por la protección de los derechos y la privacidad dentro de sus fronteras.

En la segunda parte del discurso, el presidente expone su posición y sus propuestas frente a la situación internacional de la ciberseguridad. Putin (2018) afirma:

> Como otros países, Rusia también enfrenta estos desafíos. Por ejemplo, el número de ataques cibernéticos en sitios web rusos en el primer trimestre de este año creció un tercio en comparación con el mismo período del año anterior…Creo que es tarea del estado neutralizarlos y brindar seguridad cibernética en general; Para resolverlo, debemos unir esfuerzos de las agencias policiales, empresas, organizaciones públicas y ciudadanos.

Posteriormente, Putin expone unas iniciativas específicas diseñadas para combatir la ciberdelincuencia que están siendo implementadas en Rusia:

- Crear soluciones integrales para prevenir y detener la ciberdelincuencia, estas soluciones deben darles agencia a los organismos encargados de imponer las leyes para responder las amenazas. Esto a través de la creación de un marco legal que brinde herramientas para una interacción más efectiva entre los individuos y las agencias gubernamentales.
- Implementar la iniciativa promovida por las empresas para crear un sistema automatizado para el intercambio de información sobre amenazas digitales. De esta manera se mejorará la coordinación entre las diferentes partes privadas con las agencias de aplicación de la ley para abordar cualquier amenaza emergente.
- Garantizar que el software y la infraestructura de comunicaciones estén basados en tecnología y soluciones rusas que hayan sido debidamente certificadas y aprobadas. Putin afirma además que con seguridad estos son productos competitivos que cumplen las expectativas de los consumidores.
- Lograr un avance de calidad en la capacitación de expertos en la lucha contra la ciberdelincuencia y para esto, se introducirán enfoques orientados a la prácticas internacionales y rusas.

- Desarrollar y mejorar los intercambios internacionales de información sobre delitos informáticos. “El Gobierno decidirá en un futuro próximo sobre la agencia que estará a cargo de este trabajo” (Putin, 2018).

Más adelante el mandatario ruso se refiere a la cooperación internacional, y afirma que esta es necesaria para lograr un consenso en cuanto a las reglas internacionales de ciberseguridad. Sin embargo, expone que se deben tener en cuenta los intereses en común y que Rusia es un referente para el tema en cuestión y la solución de disputas en este. Entonces se convierte en un modelo de cooperación en el cual Rusia debe ser el referente central y esto ya no sería cooperación sino imposición. En este punto también habla de la libertad, pero a diferencia de la primera parte del discurso, se refiere a la naturaleza anárquica del ciberespacio más que a la libertad para el bienestar común. Putin aseguró:

> Hemos visto más de una vez que el egoísmo y las políticas egocéntricas de algunos países están dañando la estabilidad de la información internacional... Rusia siempre ha pedido una solución justa y conjunta de cualquier problema que surja…Al mismo tiempo, creemos que las medidas de seguridad y la regulación de este espacio no deben obstaculizar su desarrollo tecnológico e innovador…Como ya dije, nuestra era digital turbulenta depende de la libertad, incluida la libertad para comunicarse, así como para intercambiar experiencias e ideas. (Putin, 2018)

Finalmente, en su discurso, el mandatario concluye reafirmando la importancia geopolítica de Rusia y cómo el país ha promovido iniciativas sobre las reglas de “comportamiento responsable de los Estados en el ámbito de la información”, así como mecanismos legales para combatir la ciberdelincuencia.

Entonces, del discurso analizado anteriormente se puede concluir principalmente que Rusia está trabajando actualmente para mejorar sus capacidades en el ciberespacio tanto a nivel nacional como internacional. A nivel nacional con la finalidad de mejorar la calidad de vida de sus ciudadanos, y a nivel internacional con la finalidad de posicionarse como el referente principal para la creación de normas para el ciberespacio.

No se puede negar la enorme influencia y poder que Rusia posee actualmente en el área, pero este es resultado del manejo de sus capacidades en el ciberespacio a través de los años. Y esta influencia no solo se denota en los discursos, sino que también se pone en evidencia

con sus acciones. En cuanto a la narrativa internacional se encuentran diferentes ejemplos que pueden evidenciar cómo se aplica dicha narrativa en la práctica.

El principal ejemplo es el ataque cibernético que sufrió Estonia en el año 2007, el cual provocó que entidades gubernamentales, bancarias y demás infraestructuras importantes quedaran bloqueadas parcial o totalmente. A pesar de no existir las pruebas suficientes para demostrar la acusación, las autoridades de Estonia declararon responsable a Rusia del ataque a partir de los datos de las terminales de procedencia del ataque (McGuinness, 2017).

Un segundo caso tuvo lugar en el año 2008, en este caso Rusia combinó sus operaciones armadas con las cibernéticas e hizo uso de estas en el conflicto armado que enfrentó contra Georgia. El país recibió ataques de denegación de servicios procedentes de Rusia, lo cual provocó que los principales sitios web del gobierno, de los bancos y de los principales medios de comunicación quedaran bloqueados. A pesar del contexto y las evidencias, en este caso tampoco se pudo demostrar la culpabilidad de Rusia, aunque con certeza se estableció que los ataques fueron realizados por un actor estatal, debido a la fuerza del mismo (El Tiempo, 2008).

Un tercer ejemplo se halla en Ucrania. El 23 de diciembre del 2015, las autoridades del país denunciaron un ciberataque a diferentes centrales eléctricas, lo que dejó sin electricidad a más de 103 ciudades y 230.000 personas. En este caso Ucrania solicitó ayuda internacional para llevar a cabo una investigación forense para encontrar al responsable de los ataques, los cuales fueron calificados de sin precedentes pues fueron capaces de penetrar infraestructuras críticas de producción y distribución de energía eléctrica sin dificultad. Al finalizar las investigaciones, Ucrania le atribuyó la responsabilidad del ataque a Rusia y lo acusó del diseño del programa maligno denominado “BlackEnergy”. Sin embargo, no hubo evidencias suficientes para atribuir el ataque al gobierno ruso (Cherepanov & Lipovsky, 2016).

Finalmente, el ejemplo más reciente es el de los ciberataques elaborados por el gobierno ruso para influir en los resultados de las elecciones presidencias estadounidenses del 2016. La diferencia con los casos anteriores es que sí se realizó una acusación; el 7 de octubre del 2016 Estados Unidos acusó oficialmente a Rusia de interferir en el proceso electoral a través del ataque cibernético dirigido al Partido Democrático y a Hillary Clinton, revelando

información crítica de estos objetivos y poniendo en riesgo además el sistema electoral. Según Gazapo (2017):

> El JAR, titulado como "Grizzly Steppe", permitió a la comunidad de inteligencia americana atribuir la autoría de los ataques cibernéticos a la Russian civilian and military Intelligence Service (RIS). En el texto se apunta que la inteligencia rusa no sólo había atacado al Partido Demócrata, sino que también había atacado a otras infraestructuras críticas, empresas, think tanks, universidades y otros actores de la sociedad. El FBI y el DHS añaden que la inteligencia rusa intentó enmascarar los ataques para torpedear las investigaciones forenses destinadas a identificar la autoría de los ataques cibernéticos. (p. 3)

En los casos anteriores se puede evidenciar que las acusaciones contra Rusia no se realizan de manera directa u oficial para evitar tensiones diplomáticas y generar más ataques cibernéticos, pero en este caso la acusación se hace directamente.

Para concluir, se puede inferir desde las evidencias y el discurso, que Rusia tiene una posición de gran poder e influencia en el tema del ciberespacio, y que cada vez realiza ataques más grandes sin temor a las consecuencias; además, que Rusia promueve constantemente su narrativa en espacios internacionales y que constantemente está aumentando sus capacidades. Finalmente, podemos evidenciar que Rusia instrumentaliza al individuo, ya que en su discurso, Putin afirma que todos los esfuerzos que Rusia está realizando para aumentar sus capacidades son "en fin del bienestar común de los ciudadanos y el desarrollo mundial", pero posteriormente denota su capacidad de liderazgo y afirma que aunque debe haber cooperación, Rusia debe ser un referente en la creación de un marco legal internacional del ciberespacio; esto y el accionar del país deja en evidencia las verdaderas intenciones que son en busca del poder y el status.

3.3 China

La narrativa de ciberseguridad de China no comparte la línea base de pensamiento de la de EE. UU, debido a que la idea de protección de datos y privacidad no es un componente en la narrativa nacional o internacional. De manera interna China no reconoce el derecho a la privacidad ni a la propiedad privada. Internacionalmente, la narrativa de China promueve el respeto a la soberanía del ciberespacio de cada Estado. En ese orden de ideas, está dispuesto

a entender una especie de ente regulador internacional, haciendo la salvedad que no está de acuerdo en que dicho ente provenga de EE. UU.

En cuanto a la narrativa internacional, China ha promovido la denominada "soberanía de Internet" como su discurso para la gobernanza del ciberespacio. Esta se promueve como una posición normativa, pero según Zeng, Stevens y Chen (2017), este discurso contiene varias formulaciones fragmentadas e incoherencias dentro de su definición y limitación. Los autores mencionados atribuyen estos problemas principalmente al patrón de formulación de políticas internas chinas, y sostienen que un discurso interno subdesarrollado ha restringido la capacidad de China para proporcionar normas alternativas en el ciberespacio.

China es el régimen autoritario más grande en el mundo y el que más usuarios de internet posee debido a su población. Estos factores, combinados con la creación de una estrategia de gobernanza global y una influencia internacional poderosa, exponen cómo China ha logrado convertir el ciberespacio en una herramienta para promover sus ambiciones políticas. El uso autoritario de China de la gobernanza de Internet tiene ciertas implicaciones políticas a considerar. Aunque se ha mostrado cooperativa y pacífica, así como su ascenso internacional, China también se ha mostrado determinada y capaz de exportar sus normas relativas a la gobernanza global para reformar las leyes internacionales del ciberespacio.

En el discurso dado por Xi Jinping en 2015 en el marco de la Conferencia mundial de Internet en Wuzhen, el mandatario chino sentenció:

> Para promover reformas en la gobernanza global del ciberespacio, debemos insistir en los siguientes principios: primero, respetar la soberanía de Internet. El principio de igualdad soberana consagrado en la Carta de las Naciones Unidas es una de las normas básicas en las relaciones internacionales contemporáneas. Cubre todos los aspectos de las relaciones de Estado a Estado, que también incluyen el ciberespacio (...) Debemos respetar el derecho de cada país a elegir independientemente su propio camino de desarrollo cibernético y modelo de regulación cibernética y participar en la gobernanza internacional del ciberespacio en pie de igualdad.

En este discurso podemos evidenciar los pilares principales de la propuesta China para la gobernanza del ciberespacio: soberanía, igualdad y autonomía para cada país en el uso del ciberespacio.

Así, la denominada “soberanía cibernética o de internet” se posicionó como un concepto de importancia a partir del referido discurso del presidente chino Xi Jinping en la Conferencia Mundial de Internet patrocinada por Beijing en Wuzhen en 2015. Bajo el liderazgo de Xi Jinping, China ha iniciado la promoción de una serie de conceptos normativos y estratégicos para aumentar su poder e influencia discursiva, realizando considerables esfuerzos para transformarse en un creador de normas. También se evidencia una mayor ambición por legitimar sus actividades coercitivas domésticas en el ciberespacio, así como el desarrollo de una posición normativa que respalde la política exterior y los intereses de China en el exterior. Sin embargo, los autores afirman que esta ambición no ha podido ser alcanzada debido a las fallas internas del discurso. Es decir, el concepto y el discurso interno tiene fallas y es por esto por lo que no se ha logrado exportar de manera exitosa. Zeng et al. (2017) aseveran:

> En este contexto, se ha promulgado la soberanía de Internet a nivel mundial para legitimar la gestión social interna del ciberespacio en Beijing y sus intentos más amplios de gobernar Internet. También forma parte de la estrategia de marketing político de China para construir un poder blando para el régimen autoritario. Además, China está pidiendo apoyo para afirmar la soberanía nacional en el ciberespacio. En el ámbito mundial, hay un debate más amplio en la gobernanza cibernética para saber si el ciberespacio debe ser globalizado o subordinado a las preocupaciones nacionales y territoriales. (p. 10)

Para comprender mejor el concepto de “la soberanía de internet” se debe analizar su definición y se debe tener una mejor comprensión de la política y el discurso interno de China sobre el ciberespacio. Zeng et al. (2017) recopilan varios textos y exponen una definición del concepto que se compone de varios elementos: el control de la información transfronteriza, la regulación y gestión de la forma en que la información fluye dentro y fuera del país, así como la jurisdicción sobre las controversias que surgen en este contexto.

En resumen, se define como “la capacidad del estado para "proteger", "gestionar" y "regular" información”. Además, entre los estudios académicos hay consenso en cuanto a dos aspectos del concepto: primero, es relativamente nuevo y por lo tanto su definición no está clara. Esto lo atribuyen en parte a la falta de claridad de los líderes políticos chinos al

momento de presentar una política o idea nueva. Y segundo, la soberanía de internet se entiende como un medio a través del cual China defiende y preserva sus intereses nacionales.

Sin embargo, en China no hay consenso en cuanto la validez y aplicabilidad del concepto de la soberanía de internet. En oposición está la narrativa liberal, la cual argumenta que este concepto "representa un intento de tolerar el control estatal de los derechos de las personas a acceder y usar Internet y afecta a la libertad de expresión" (Zeng et al., 2017, p. 12). Contrario a lo anterior, la posición general en China argumenta que la soberanía de la información refleja la soberanía nacional en la actividad cibernética y por lo tanto es necesaria. Para comprender esta posición debemos analizar el discurso y la política que China maneja a nivel nacional.

Como régimen autoritario, China reconoce la preocupación por los posibles efectos de catalizadores de internet y otras tecnologías de información y comunicación en la desobediencia civil y la disidencia en masa. Según cifras del China Internet Network Información Center (2016), para el 2016 eran 688 millones de chinos usuarios de internet (como se citó en Sputnik, 2016), convirtiéndose en la comunidad de cibernautas más grande del mundo. Es por esto por lo que la política nacional de China sobre el ciberespacio se basa en una poderosa estrategia del gobierno para la prevención y contención del acceso a ideas potencialmente desestabilizadoras.

El gobierno empezó a desarrollar e implementar "el Proyecto Golden Shield" desde finales de los 1990. Este programa posee una matriz de vigilancia técnica, bloquea el acceso a recursos de internet en la lista negra, y censura las palabras clave y frases prohibidas en el tráfico de la red. Por lo tanto, los usuarios tienden a seguir las leyes porque son conscientes de la efectividad del sistema y las consecuencias en cuanto a medidas legales y reglamentarias en caso de infringir estas leyes (Zeng et al., 2017).

Por ejemplo, en el año 2011, durante el punto máximo de la Primavera Árabe, se creó un movimiento paralelo anónimo denominado "Revolución de los Jazmines" que llamaba a la oposición en China. El gobierno tomó medidas inmediatas para judicializar a los activistas de derechos humanos y disidentes, así como la censura en línea del término "jazmín" y

“primavera árabe”, y el despliegue de policía para reprimir las protestas populares (Zeng et al., 2017).

Adicionalmente, hay un segundo ejemplo en 2013, después del golpe militar en Egipto, el gobierno chino realizó esfuerzos a través de la maquinaria de propaganda para vincular los movimientos de democratización en Medio Oriente con el caos en el país; de esta manera, la estrategia del gobierno fue legitimar su sistema al desacreditar a la democracia liberal, entonces los términos que anteriormente eran tabú (como jazmín o Primavera Árabe) se convirtieron en blanco de burla en los medios de comunicación estatales de China (Alhindi, Talha, & Sulong, 2012).

Además, se debe tener en cuenta que las reformas de mercado que se realizaron en China sentaron las bases para la situación económica actual del país, pero también aumentaron la brecha entre ricos y pobres. Frente a esto, las tecnologías de información y comunicación han permitido a la población china una alternativa para encontrar y difundir información contraria a las narrativas estatales. Sin embargo, el gobierno ha logrado responder a estas nuevas amenazas con la implementación de regulaciones (Zeng et al., 2017).

Teniendo en cuenta el análisis anterior es posible concluir que la posición internacional de China se basa en el concepto de “soberanía de internet”, en tanto que busca legitimar sus políticas internas, y aunque acepta la posible creación de un ente regulador, este sería únicamente para las relaciones entre Estados, mas no tendría autoridad en las políticas internas del ciberespacio de cada país. Claramente, la privacidad y el derecho de los individuos no se encuentra como una preocupación en el discurso de China y no hay un respeto por estos.

4. SECURITIZACIÓN DEL CIBERESPACIO: ESTADOS UNIDOS

El fin de la Guerra Fría y el orden internacional bipolar produjo un cambio en la noción de la seguridad, pues este dejó de comprenderse únicamente en términos militares. Las tecnologías de información y comunicación (TIC) fueron claves en la Guerra Fría y, desde entonces, se incorporaron como parte crucial de la guerra y la seguridad de los Estados (Klingova, 2013).

Esto, sumado a los procesos de globalización y tecnificación de la sociedad humana, representó una extensión del sector militar y un cambio en el concepto tradicional de seguridad, el cual se reformuló en un enfoque más holístico y menos estatocéntrico. Las especificaciones de quiénes son los sujetos y amenazas de seguridad empezaron a generar debate. Es en este punto que se empiezan a incluir temas en la agenda de seguridad y comienza el proceso de securitización (Klingova, 2013).

La teoría de securitización de la Escuela de Copenhague es específicamente adecuada para el ciberespacio debido a su comprensión de la seguridad como una modalidad discursiva con una estructura retórica y efectos políticos particulares. Además, esta señala que el discurso de seguridad comprende otros objetos referentes distintos al Estado, lo cual aplica perfectamente en el ciberespacio, en donde individuos, Estados, empresas privadas y demás actores se relacionan (Klingova, 2013).

Sin embargo, este proceso de securitización no sucede de un día para otro, es por esto que a continuación se analizan diferentes periodos de tiempo en los cuales es posible evidenciar la evolución del discurso de Estados Unidos sobre el ciberespacio.

4.1 El primer periodo comprende desde 1997 hasta el 2001

Este periodo se caracteriza por el boom de la "world wide web", es decir, la red de internet. Es la época en que el internet se vuelve popular y las personas se encuentran asombradas de la información disponible por este medio. Esto sucede durante el segundo mandato de la administración Clinton, cuyo gabinete reconoce de inmediato que la interconectividad a pesar de todos sus beneficios crea vulnerabilidades para el gobierno y los individuos. Es por esto por lo que Clinton dio roles más amplios a expertos y líderes de la industria a través de colaboraciones público-privadas en la gestión de riesgos y vulnerabilidades en "la infraestructura crítica de la información". Dicho concepto de la infraestructura crítica se define durante la administración Clinton como aquellos sistemas físicos y cibernéticos esenciales para las operaciones mínimas de la economía y el gobierno. Schwarz (2016) afirma que:

> La Administración se basó en gran medida en la evaluación de las implicaciones futuras que podría tener el espacio en los objetos de referencia colectiva; como la seguridad nacional, el estado y la economía a través del desarrollo de infraestructura crítica. En otras palabras, las amenazas se presentaron como de futuro, lo que limitó temporalmente la securitización del ciberespacio ya que las amenazas no fueron inmediatas. (p. 12)

Esto quiere decir que el proceso de securitización no se da en este momento porque en este contexto no se entiende el ciberespacio como una amenaza existente que necesite una respuesta excepcional. Entonces, no se utilizaron análisis de política exterior o seguridad nacional, sino que se les dio un rol importante a los científicos informáticos para calcular las amenazas cibernéticas. Esto dio como resultado la tecnificación del ciberespacio.

En octubre de 1997 se presenta "El informe de la Comisión del Presidente sobre Infraestructura Crítica", este documento ayudó a conectar el ciberespacio a la seguridad nacional a través del concepto de infraestructura crítica de la información. Sin embargo, el documento no presenta el ciberespacio como un riesgo inmediato, sino que meramente lo conceptualiza en términos de amenaza y presenta cómo puede ser manejado por expertos técnicos.

Este mismo año se realizó un ejercicio militar conjunto denominado "Receptor Elegible", el cual buscaba probar las capacidades de planificación y acción de Crisis del Departamento de Defensa (DoD) ante ataques a infraestructuras de información. El DoD no estaba enterado de la realización del ejercicio por lo que los comandos militares y agencias gubernamentales reaccionaron de manera real a los ataques. En esta simulación de un ataque cibernético a gran escala, el DoD se dio cuenta de que era necesario tomar medidas para estar mejor preparados (Schwarz, 2016).

Es por esto que Clinton estableció la "Comisión del Presidente sobre Protección de Infraestructura Crítica" (siglas en inglés: PCCIP). Esta comisión estaba compuesta principalmente por especialistas y agencias de poder ejecutivo, junto con representantes de la industria privada y académica. La misión de la PCCIP era de abordar los riesgos a la infraestructura crítica. El equipo de expertos compiló una evaluación de las vulnerabilidades y riesgos potenciales a las infraestructuras de información y recomendó la creación de una política nacional y una estrategia (Schwarz, 2016).

El informe entregado por la PCCIP estableció que la tecnología es una causa potencial de amenaza, pero también es un medio para gestionar riesgos futuros. Entonces, la narrativa que se desarrolla en este contexto expone al ciberespacio como una amenaza que debe ser manejada para que en el futuro no se convierta en una amenaza existencial. El informe afirmó que en ese momento no se encontraban amenazas, pero que definitivamente existe la capacidad generalizada para explotar las vulnerabilidades de la infraestructura crítica y que se debían desarrollar mejores defensas para el futuro. Como resultado, a los expertos técnicos se les otorgó una posición privilegiada para definir agendas e imponer premisas en los discursos. Schwarz (2016) argumentó:

> Como resultado de la incertidumbre, los expertos están acostumbrados a crear narrativas de y sobre riesgos. que luego ponen a disposición del público en general. En otras palabras, los expertos están autorizados para articular qué y cómo están surgiendo los riesgos en nombre del público (…) En la década de 1990, las amenazas cibernéticas a estas infraestructuras eran bastante nuevas. La Comisión enfatiza la complejidad técnica de los riesgos porque hace que la construcción esté menos disponible. La complejidad técnica reduce la autoridad para calificar el riesgo a los expertos técnicos. Ciertamente, esto puede ayudar a disipar los conceptos erróneos sobre el riesgo. (p.21)

Entonces, en este periodo la autoridad del ciberespacio pasa de los formuladores de políticas a los informáticos y el personal técnico, esto quiere decir que se les concedió el poder sobre asuntos técnicos y políticos del ciberespacio. La tecnificación y la caracterización del ciberespacio como riesgo fueron características propias de este periodo. La narrativa frente al ciberespacio se basaba en amenazas anticipadas, por lo tanto, aún no se enmarcaba como un tema en la agenda de seguridad. Sin embargo, después de los acontecimientos del 11 de septiembre de 2001 esta narrativa cambiaría.

4.2 El segundo periodo comprende desde el 2001 hasta el 2005

En este contexto es posible identificar el comienzo de la securitización, debido a que los acontecimientos del 9/11 desencadenaron una serie de medidas de respuesta excepcionales, entre ellas la reformulación de conceptos esenciales como la “seguridad”, la creación de instituciones y leyes sobre el ciberespacio sin precedentes, entre otras medidas que se

expondrán a continuación. Definitivamente se evidencia un cambio en el discurso y la narrativa de Estados Unidos sobre el ciberespacio. Este periodo se caracteriza porque el ciberespacio se convierte en un tema de la agenda de seguridad en todos los países. En Estados Unidos, particularmente, es en este contexto se crean las instituciones, leyes, y documentos oficiales que contienen la base del discurso de ciberseguridad.

Los acontecimientos del 11 de septiembre de 2001 cambiaron la agenda y el discurso de seguridad en Estados Unidos no solo en el campo del ciberespacio. El "terrorismo" se estableció como una amenaza inmediata que podría usar cualquier medio para socavar los intereses del país. El ciberespacio ya no podría ser visto como una amenaza distante, sino que ahora es considerada un amenaza existente e inmediata, y un potencial medio para que los terroristas realicen ataques al país.

Para el 2001 se encontraba de turno la administración de Bush, la cual tomó medidas inmediatas. En primer lugar, se recurrió a los tecnólogos por varias razones: al convertir el ciberespacio en un tema técnico se lograba apartarlo del público general, debido a que sus conocimientos estaban más allá de la comprensión del común. Además, al categorizarlo como un tema técnico y tecnológico se excluye al usuario, al componente humano, exhortando la idea de que las medidas tomadas son apolíticas y amorales. Finalmente, la tecnificación infundió la percepción de que la amenaza puede ser racionalizada y cuantificada, debido a que los expertos prometían identificar vulnerabilidades y garantizar la seguridad.

Todo esto llevó a que el gobierno otorgara cierta autoridad en el tema a los expertos técnicos para garantizar la seguridad y promover el discurso de conveniencia para el gobierno. Dichos expertos, presentaron en octubre de 2001 el "USA Patriot Act", con el objetivo de fortalecer las medidas de seguridad contra el terrorismo a través de la expansión de los poderes de las agencias policiales y federales (FBI, CIA, NSA, y las fuerzas armadas norteamericanas) a los efectos de obtener información confidencial.

"USA Patriot Act" es un acrónimo para "*Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act*", lo que en español traduce "Ley para unir y fortalecer Estados Unidos, proveyendo las herramientas apropiadas

para impedir y obstaculizar el terrorismo". En esta ley el Congreso incluyó disposiciones que facilitan la vigilancia de las actividades de internet por parte de las autoridades estadounidenses. Estas disposiciones se encuentran en la sección del "Título II: Procedimientos de vigilancia mejorados, incluyendo disposiciones que afectan la supervisión de las actividades de internet" (Smith, Seifert, McLoughlin, & Dimitri, 2002). Algunas de las disposiciones más controversiales del "USA Patriot Act" incluyen:

- La Sección 210 amplía la información que los funcionarios encargados de hacer cumplir la ley pueden obtener (con la autorización apropiada) de los proveedores de servicios de comunicaciones electrónicas o servicios de computación remota con respecto a un suscriptor o cliente de esos servicios. La información ahora puede incluir los medios de un suscriptor o cliente y la fuente de pago.
- La sección 211 dispone que las compañías de cable que ofrecen servicios de internet están sujetas a intercepción de cables y dispositivos electrónicos e intercepción de comunicaciones orales; acceso a la información almacenada por cable, por comunicaciones electrónicas y registros de transacciones; y, acceso a registros de dispositivos de captura y rastreo. Sin embargo, la sección 202 y 217 aclara que los funcionarios encargados de hacer cumplir la ley deben solicitar permiso para interceptar las comunicaciones electrónicas de los "intrusos informáticos".
- La Sección 217 le permite a una persona que actúa bajo la ley interceptar el cable o las comunicaciones electrónicas de un intruso informático transmitido a través de, o desde una computadora protegida bajo ciertas circunstancias.
- La Sección 220 permite las órdenes de búsqueda en todo el país para el correo electrónico en lugar de requerir órdenes de búsqueda por separado para cada jurisdicción en la que se pueda ubicar el correo electrónico, como en la ubicación del ISP en lugar de donde se cometió un delito (Smith et al., 2002).

Así pues, es importante comprender que antes del 9/11 el debate sobre la privacidad de los usuarios en el ciberespacio se centró en los problemas provocados por parte de operadores comerciales en los sitios web. Sin embargo, las prácticas de los organismos encargados de hacer cumplir la ley en la supervisión de las actividades de los usuarios en internet era un

problema menos visible. Debido a las disposiciones que el Congreso en el "USA Patriot Act" para facilitar la vigilancia de las actividades de internet por parte de las autoridades estadounidenses, posteriormente se inclinó el debate hacía las prácticas de los organismos gubernamentales encargados de la supervisión del ciberespacio.

En el "USA Patriot Act" además se establece una definición más amplia de la "infraestructura crítica de la información". Este concepto durante la administración de Clinton se definió como "los sistemas físicos y cibernéticos esenciales para el gobierno". Durante la administración de Bush esta definición se amplió abarcando:

> Los sistemas y activos, ya sea físicos o virtuales, tan vitales para los Estados Unidos que la incapacidad o destrucción de tales sistemas y activos tendría un impacto debilitante en la seguridad, ya sea económica, de salud o seguridad pública nacional, o cualquier combinación de esos asuntos. (Schwarz, 2016, p.34)

Es decir, el concepto de "infraestructura crítica" se amplió de los sistemas que garantizaban el funcionamiento mínimo del gobierno y la economía, a todos los sistemas y activos que tienen impactos en la seguridad.

En dicha definición se puede ver claramente la instrumentalización del individuo en la medida en que el concepto no solo expone la infraestructura crítica como un elemento vital para el funcionamiento de los sistemas de información del país, sino también para los individuos estadounidenses, para su seguridad e incluso para el mantenimiento de su estilo de vida. De esta manera se conecta el ciberespacio directamente con la seguridad nacional. Consecuentemente, el ciberespacio se considera como derecho propio. Sin embargo, se debe tener en cuenta que el ciberespacio se securitizó en una dicotomía en la cual representa una amenaza, pero a la vez es visto como un objeto referente que necesita ser protegido.

Entonces, el ciberespacio se presenta en el documento como el sistema nervioso de las infraestructuras del sistema de control de Estados Unidos. Por lo tanto, el funcionamiento del ciberespacio se expone como esencial para la economía y seguridad nacional. No obstante, esta definición dada del ciberespacio es técnica, y, de nuevo, no tiene en cuenta a los usuarios ni sus libertades y en general omite el componente humano en el ciberespacio, exponiéndolo

meramente como una infraestructura. Esta definición omite el hecho de que las decisiones tomadas frente al ciberespacio afectan a los usuarios.

Complementando el "USA Patriot Act", en el siguiente año (2002) se creó la Oficina de Seguridad Nacional, que un año después se convirtió en el Departamento de Seguridad Nacional (Homeland Security, DSN), cuya misión explícita es proteger a Estados Unidos de ataques terroristas. Como parte de esta misión la DSN es la encargada de proteger la infraestructura crítica de la información tanto pública como privada. La creación del DSN representó, según la página oficial del referido departamento:

> La transformación más significativa del gobierno de los Estados Unidos en más de medio siglo, al modificar y realinear en gran medida el actual mosaico confuso de las actividades del gobierno en un solo departamento cuya misión principal es proteger la patria. (Homeland Security, 2002, párr. 5)

En el documento oficial en el cual Bush propone la creación del DSN, se afirma de manera explícita que este hace parte de la respuesta a los acontecimientos del 9/11, y que el objetivo del departamento es asegurar la libertad y la democracia. En el documento oficial Bush (2002) expresa lo siguiente:

> Los ataques del 11 de septiembre resaltaron el hecho de que los terroristas son capaces de causar un daño enorme a nuestro país al atacar nuestra infraestructura crítica, esos activos, sistemas y funciones vitales para nuestra seguridad nacional, gobernanza, salud pública y seguridad, economía y moral nacional (…) Esta propuesta refleja plenamente el compromiso absoluto del Presidente de salvaguardar nuestra forma de vida, incluida la integridad de nuestro sistema político democrático y los elementos esenciales de nuestra libertad individual.

Posteriormente, para apoyar la gestión del DSN se creó la Junta de Protección de Infraestructura Crítica del Presidente (PCIPB, por sus siglas en inglés) y el Consejo Consultivo de Infraestructura Nacional (NIAC, por sus siglas en inglés). Estas eran organizaciones conformadas por expertos miembros del sector privado, academia y gobierno estatal/local.

En todos los documentos oficiales constitutivos de las organizaciones anteriormente mencionadas y el "USA Patriot Act" se expone y consolida el discurso de ciberseguridad de Estados Unidos, ya que en dichos documentos se reformuló la relación entre el ciberespacio y la seguridad nacional.

De esta forma, se aprecia que el discurso expone la identidad de Estados Unidos como defensor de la libertad y los derechos individuales, lo cual posiciona al individuo como el centro del discurso. Todo esto a pesar de que evidentemente los riesgos de ataque cibernético a la infraestructura crítica estaban siendo generados principalmente por otros Estados y no por individuos.

En 2003 el DSN entregó los informes denominados "Estrategia Nacional para Asegurar el Ciberespacio" y "Estrategia nacional para la protección física de infraestructuras críticas y activos clave", en los cuales se afirma que el gobierno federal y la sociedad a partir del 9/11 se vieron en la necesidad de reexaminar las ideas de seguridad del país. Como resultado, las vulnerabilidades de la infraestructura de la información ya no se evaluarían como amenazas futuras, sino que debían protegerse como una amenaza activa. Además, el informe afirma que la economía y la seguridad nacional de los EE. UU. se volvieron totalmente dependientes de la tecnología y la infraestructura de la información en la que se ejecuta. Consecuentemente, el ciberespacio se convierte en algo vital para la seguridad de Estados Unidos. Schwarz (2016) enuncia:

> A través de esta caracterización, las amenazas presentadas por el ciberespacio son técnicas, pero cada vez más urgentes. Además, la Estrategia Nacional para Asegurar el Ciberespacio enmarca el diseño del ciberespacio e Internet como una amenaza para las infraestructuras críticas. Si bien este marco presenta al ciberespacio como una amenaza, también hace que la fuente de la amenaza sea técnica y, por lo tanto, no esté disponible para el público. Además, ignora el elemento humano del ciberespacio, los usuarios. A través de este encuadre, la discusión ocurre en términos de tecnología a pesar del hecho de que tienen implicaciones más allá. Por lo tanto, la securitización se basa en la tecnificación para crear la amenaza. Dentro de la Estrategia Nacional para Asegurar el Ciberespacio, el ciberespacio se presenta como una amenaza técnica para la infraestructura crítica. (p. 32)

El informe además describe el internet como un sistema que fue originalmente diseñado para compartir investigaciones no clasificadas entre científicos, pero que actualmente conecta a millones de redes necesarias para el funcionamiento de los servicios e infraestructuras esenciales de la nación. Esto implica que no se esperaba tal expansión en el alcance de internet y por lo tanto representa una amenaza para el gobierno y los usuarios.

Como medida adicional, se realizaron paneles entre los expertos y la población común en donde se les presentaba las amenazas del ciberespacio al público y se exponía cómo ellos podrían enfrentarlas. Estos espacios permitieron a los estadounidenses discutir este tema tan importante pero también fue un espacio para presentar la narrativa al público. Esto demuestra que la "Estrategia Nacional para Asegurar el ciberespacio" fortaleció la securitización a través de la tecnificación del ciberespacio, la cual a su vez brindó un sentido de legitimidad y neutralidad política al proceso, por ser presentado al público por expertos técnicos y no políticos.

En conclusión, este periodo se caracterizó por ser el comienzo de la securitización. Proceso que se da como respuesta a los acontecimientos del 9/11. En este contexto se consolida el discurso de ciberseguridad estadounidense y posteriormente se divulga al público. Dicha securitización se logró a través de la reformulación de conceptos, la creación de instituciones y leyes, pero más importante, la divulgación por parte del gobierno del discurso que justifica la necesidad de aumentar sus capacidades para mantener la seguridad de los individuos y cumplir su rol de defensor de derechos y libertades en el sistema internacional.

Sin embargo, en los elementos analizados anteriormente como el Patriot Act, la misión del DSN y sus funciones, así como la extensión de poderes de agencias gubernamentales para la "supervisión de actividad cibernética", se observa que las acciones propuestas por el gobierno implican un irrespeto por el derecho a la privacidad de los usuarios.

4.3 El tercer periodo comprende desde 2005 hasta el 2017

La administración de Bush continuó con la misma narrativa hasta el final de su mandato en 2009, año en el que comienza la administración de Obama, la cual comprende hasta el

2017. El último documento sobre el ciberespacio de gran importancia entregado durante la administración de Bush fue la Iniciativa Nacional de Seguridad Cibernética (CNCI) de enero de 2008, la cual sirvió como base para las posteriores iniciativas planteadas durante la administración de Obama (Schwarz, 2016).

La narrativa en los años posteriores a la administración de Bush continuó con las bases con las que se creó y consolidó. Sin embargo, teniendo estas bases consolidadas, las administraciones posteriores hicieron especial énfasis en la legitimación de esta narrativa a nivel internacional. Lo que cambió a través de los años fueron los argumentos para dicha legitimación. En principio se enfatizó en el argumento de que Estados Unidos, por ser el pionero en el desarrollo de internet, tenía por derecho la soberanía del ciberespacio y que esta no era una afirmación política debido a que se trata de un tema técnico (siguiendo con la tecnificación como argumento de neutralidad) (Schwarz, 2016).

Posteriormente, dicho argumento pasó a un segundo plano y se hizo énfasis en la declaración de Estados Unidos de ser el país más apto para generar las normas de derecho internacional para la gobernanza del ciberespacio, debido a los principios y valores de libertad del país. Es en este contexto que más se evidencia la instrumentalización del individuo y sus libertades como justificación para la toma de decisiones y medidas escaladas para la "seguridad" del ciberespacio. Es por esto que los términos privacidad y libertad se repiten constantemente en los discursos del expresidente Obama sobre ciberseguridad, lo cual se verá a continuación. En su discurso enunciado el 29 de mayo de 2009 en la Casa Blanca, Obama (2009) afirmó:

> Se trata de la privacidad y la seguridad económica de las familias estadounidenses. Confiamos en Internet para pagar nuestras facturas, realizar transacciones bancarias, realizar compras, presentar nuestros impuestos. Pero hemos tenido que aprender un vocabulario completamente nuevo solo para mantenernos a la vanguardia de los ciberdelincuentes que nos harían daño: spyware y malware y suplantación de identidad, phishing y botnets. Millones de estadounidenses han sido víctimas, se ha violado su privacidad, sus identidades han sido robadas, sus vidas han sido arruinadas y sus billeteras han sido vaciadas. Según una encuesta, solo en los últimos dos años el delito cibernético ha costado a los estadounidenses más de $ 8 mil millones (…) Para garantizar que las políticas mantengan la fe en nuestros valores

> fundamentales, esta oficina también incluirá un funcionario con una cartera dedicada específicamente a salvaguardar la privacidad y las libertades civiles de los estadounidenses.

Al comenzar su mandato en 2009 Obama inició sus esfuerzos de seguridad cibernética con la "Revisión de la política del ciberespacio de 60 días", una revisión sólida sobre dónde se encontraba el gobierno en relación con la seguridad cibernética. Sin embargo, el documento no presentaba una visión clara de cómo se llegaría a las metas deseadas. La recomendación más importante que se planteó en la revisión fue designar a un único funcionario para coordinar los esfuerzos gubernamentales y nacionales. El funcionario escogido para ser el "ciber czar" fue Howard Schmidt, quien había sido asesor de ciberseguridad durante la administración de Bush (Nojeim, 2010).

Desde entonces se empezó a gestionar el plan de ciberseguridad que se iba a manejar durante la administración de Obama. No obstante, fue a partir de los ataques cibernéticos de 2014 que se empezó a generar respuestas extraordinarias como órdenes ejecutivas, creación de nuevas posiciones e instituciones gubernamentales, debido a la situación. Sucedieron varios ataques cibernéticos a empresas estadounidenses en dicho año, algunas de las afectadas fueron: ebay, JPMorganChase, The Home Depot, Anthem, entre otras. La víctima del ataque cibernético más importante del año fue la empresa "Sony Pictures", después de revelar el largometraje "The interview", el cual contiene una escena en la que se alude a la muerte del mandatario norcoreano Kim Jong-Un (BBC Mundo, 2014).

Después de recibir amenazas, el 24 de noviembre de 2014 fue hackeado un paquete de información que contenía la información de más de 12.000 correos electrónicos de la cuenta de Michael Lynton, presidente del estudio; además, se paralizaron los sistemas informáticos y se filtraron datos financieros y privados de la compañía. Posteriormente al ataque, el FBI realizó declaraciones en donde manifestaron:

> El ataque de Corea del Norte contra Sony reafirma que las amenazas cibernéticas representan uno de los más graves peligros para la seguridad nacional de EE. UU (..) Las acciones de Corea del Norte tenían la intención de infligir un daño importante en una empresa de EE. UU. y suprimir el derecho de los ciudadanos americanos a expresarse. (BBC Mundo, 2014, párr. 17)

A partir de estos acontecimientos, entre 2015 y 2017, la administración de Obama presentó tres iniciativas para mejorar la ciberseguridad en las agencias federales: El Sprint de Ciberseguridad, el Plan de Implementación de la Estrategia de Ciberseguridad (CSIP) y el Plan de Acción Nacional de Ciberseguridad (CNAP) y firmó la Orden Ejecutiva 13694. Esta administración en particular se esforzó en su discurso y acciones por mostrar la preocupación por la libertad y privacidad (Schwarz, 2016).

Por ejemplo, en 2015 Obama firmó una orden ejecutiva sobre "ciberseguridad y protección del consumidor". La cual se centró en las asociaciones público-privadas y la protección del consumidor. Durante la firma de la orden, el mandatario afirmo que (Obama, 2015)

"El mundo cibernético es una especie de Salvaje Oeste. Y en cierta medida, nos piden que seamos el sheriff" (Zezima, 2015, párr. 29) . Paralelamente, se realizó un Sprint de Ciberseguridad que duró 30 días, desde el 12 de junio de 2015. El Equipo de Sprint de Ciberseguridad ("Equipo Sprint"), dirigido por la Oficina de Administración y Presupuesto (OMB), fue compuesto por representantes del Consejo de Seguridad Nacional (NSC), el Departamento de Seguridad Nacional (DHS), el Departamento de Defensa (DoD), junto a otras agencias federales civiles y de defensa. El memo inicial de Sprint instruyó a las agencias a implementar una serie de acciones inmediatas de alta prioridad para mejorar la ciberseguridad de la información y los activos federales. La Estrategia de Ciberseguridad y Plan de Implementación ("CSIP") es el resultado del Sprint de Ciberseguridad e incorpora informes de progreso y acciones correctivas (The White House, 2016).

La finalidad del CSIP era "identificar y abordar las brechas críticas de seguridad cibernética y las prioridades emergentes, y hacer recomendaciones específicas para abordarlas". Para este fin, el CSIP plantea cinco objetivos principales: Identificación priorizada y protección de información y activos de alto valor; detección oportuna de y rápida respuesta a incidentes cibernéticos; recuperación rápida de incidentes cuando ocurren y adopción acelerada de lecciones aprendido de la evaluación de Sprint; reclutamiento y retención de la fuerza laboral de seguridad cibernética más calificada que el gobierno federal

puede aportar; y adquisición y despliegue eficientes y efectivos de sistemas existentes y emergentes (The White House, 2015).

Para complementar estas acciones, un año después, en 2016, Obama firmó una segunda orden ejecutiva estableciendo "El Consejo Federal de la privacidad" (The White House, 2016). De esta manera, se establecieron diferentes agencias y leyes que institucionalizaron el discurso. En la orden ejecutiva el presidente expresó:

> La misión del gobierno de los Estados Unidos es servir a su gente. Para cumplir su misión, el Gobierno recopila, mantiene y utiliza legalmente grandes cantidades de información sobre personas en una amplia gama de contextos. La protección de la privacidad en la recopilación y el manejo de esta información es fundamental para el cumplimiento exitoso de la misión del Gobierno. El buen funcionamiento del gobierno requiere la confianza del público, y para mantener esa confianza, el gobierno debe esforzarse por mantener los más altos estándares para recopilar, mantener y utilizar datos personales. La privacidad ha estado en el corazón de nuestra democracia desde sus inicios, y la necesitamos ahora más que nunca. (Obama, 2016, p. 12)

Esta orden ejecutiva se lanzó paralelamente con el Plan de Acción Nacional de Ciberseguridad (CNAP), el cual contiene acciones a corto plazo que se planteó en función de "mejorar las capacidades de seguridad cibernética del gobierno federal, el sector privado, y los usuarios cotidianos". Además, en CNAP se establece un presupuesto de más de $ 19 mil millones para la ciberseguridad en el año 2017, un aumento de más del 35 por ciento con respecto al nivel promulgado en 2016 (The White House, 2016).

Lo importante a resaltar sobre este periodo es el hecho de que la meta se convirtió en propagar los conceptos que se definieron durante la administración de Bush y la visión de Estados Unidos del ciberespacio, así como aumentar las capacidades del país para demostrar su idoneidad para liderar la gobernanza del ciberespacio. Esta meta se plasma implícitamente en los documentos mencionados y se justifica a través de la instrumentalización del individuo y sus libertades. Para el cumplimiento de esta meta el país comenzó la creación de alianzas con países afines a los intereses de Estados Unidos, construyendo un bloque que actualmente se está fortaleciendo para hacer contrapeso a las narrativas de China y Rusia (Schwarz, 2016).

Como se pudo evidenciar anteriormente, en el tercer capítulo numeral (a) de la presenta investigación Trump continúa con dicha meta de propagar la narrativa de Estados Unidos y fortalecer su bloque ideológico. Empero, en la actualidad estas narrativas se encuentran entre la securitización y la militarización, términos cuya línea delimitante pareciera se está desvaneciendo en las narrativas.

En conclusión y para finalizar el presente capítulo de la investigación se destacan ciertos elementos relevantes. A través del análisis histórico y discursivo de la narrativa estadounidense sobre el ciberespacio se puede evidenciar no solo el proceso de securitización del ciberespacio sino cómo este evoluciona a lo largo de cada administración. A partir de los conceptos construidos, como el de la "infraestructura crítica", la narrativa estadounidense logró presentar el ciberespacio como un tema de seguridad nacional cuya gobernanza debe ser liderada por el país y regido de manera neutra y justa, a través de los tecnólogos. Lo anterior se argumenta discursivamente con muchos elementos, pero posteriormente a la administración de Bush se hizo énfasis en el argumento de que Estados Unidos es el país idóneo para liderar dicha gobernanza debido a sus bases que respetan la libertad y privacidad de los individuos, y se señala que las demás narrativas no comparten estas bases y por lo tanto amenazan la seguridad mundial del ciberespacio.

Este argumento le ha permitido al país construir un bloque de países afines a las ideas estadounidenses. Sin embargo y a pesar de su constante repetición, el argumento del respeto de la privacidad y libertad de los individuos no se evidencia de igual manera en las acciones del país. Es por esto que se puede concluir que este argumento es meramente discursivo y por lo tanto se instrumentaliza al individuo en orden de conseguir la meta de propagar la visión estadounidense del ciberespacio y sobrepasar las capacidades de los demás países.

5. CONCLUSIONES

Esta investigación se planteó el objetivo de determinar si se instrumentaliza al individuo en las narrativas de ciberseguridad. Para lograr este objetivo se realizó en el primer capítulo una contextualización del problema que representa el ciberespacio para los Estados e

individuos debido a la ausencia de consenso frente a la gobernanza de este. Posteriormente, se analizaron las tres narrativas dominantes en el contexto contemporáneo, presentando los discursos establecidos por diferentes países y bloques; esto con el fin de identificar las similitudes y diferencias entre las narrativas y comprender lo que implica para los individuos su aplicación a nivel internacional. Seguidamente, en el segundo capítulo se analizó como caso de estudio la narrativa de Estados Unidos, dado que actualmente es la preponderante y busca establecer un bloque ideológico, a través de la instrumentalización del individuo y sus derechos. Para este análisis, se realizó una periodización, analizando el contexto histórico en el cual se identifica el proceso de securitización del ciberespacio.

Cada capítulo de la investigación arrojó conclusiones importantes que se deben mencionar. En el primer capítulo se identificó una similitud importante entre el discurso de Estados Unidos y el de Rusia, de manera que ambos subrayan constantemente la importancia de las libertades individuales y justifican sus acciones argumentando que estas son para la seguridad de sus ciudadanos y de los individuos en el mundo. Ambos países han realizado esfuerzos enormes en el desarrollo de sus capacidades cibernéticas.

Sin embargo, a la hora de exponer ¿por qué su narrativa debe ser la que lidere la gobernanza del ciberespacio? Los argumentos tienen diferentes enfoques: Estados Unidos presenta una imagen casi mesiánica, y se define a sí mismo como el protector de la libertad y la democracia; además, expone a sus competidores como enemigos de la libertad y promotores de la criminalidad cibernética. También hace énfasis en el hecho de que internet fue un proyecto que nació en Estados Unidos y por lo tanto el país tienen un derecho implícito frente al ciberespacio.

Rusia, por otro lado, además de justificar sus acciones en la seguridad y libertades de los individuos, hace énfasis en que la narrativa del país es idónea para la gobernanza del ciberespacio, dado que promueve las reglas de "comportamiento responsable de los Estados en el ámbito de la información", y que además el país es un referente en la resolución de conflictos. China, en contraste, hace énfasis en su discurso en la noción de "soberanía del ciberespacio", un término que a pesar de ser central, carece de una definición clara, lo que limita la propagación del discurso a nivel internacional. Sin embargo, el comportamiento de

China en cuanto al manejo del ciberespacio nacional evidencia la ausencia de respeto por los derechos y libertades del individuo, por lo tanto, este no es un elemento importante en su discurso.

En el segundo capítulo también hay conclusiones importantes. Teniendo en cuenta el análisis previo de las tres narrativas dominantes, se puede evidenciar que la narrativa de Estados Unidos es la más influyente actualmente y la que más elementos posee, es por esto que en el segundo capítulo se realizó un análisis histórico y rastreo de proceso de la construcción de la narrativa estadounidense. En este análisis se encontró que hubo hitos importantes históricamente que impulsaron la securitización. Los acontecimientos del 9/11 se identificaron como el primer factor relevante históricamente para comenzar el proceso de securitización. Es en este contexto histórico (2001) que se realizan una serie de acciones extraordinarias como respuesta al incidente, algunas de estas acciones incluyeron una redefinición de conceptos, atribución de autoridad a los técnicos, creación de leyes e instituciones. Las administraciones posteriores realizaron algunos cambios mínimos, pero en general se continúa difundiendo los lineamientos establecidos desde la administración Bush con el objetivo de crear un bloque ideológico compuesto por Estados, académicos, instituciones y organizaciones. Actualmente se evidencia un punto crítico en la historia, se puede ver que el discurso se ha intensificado, llegando a señalar y acusar a sus competidores de promotores del crimen cibernético, y la administración Trump ha afirmado que está dispuesta a utilizar los recursos e impartir los castigos necesarios para “defender” el ciberespacio.

A partir de lo encontrado, la conclusión presentada es que afirmativamente se instrumentaliza al individuo en las narrativas de ciberseguridad. Sin embargo, se debe aclarar que debido al planteamiento y marco de la investigación, esta conclusión se refiere al objeto estudiado, es decir, el discurso. Debido a los limites, y aunque se incluyeron algunos ejemplos prácticos del uso del discurso, el alcance de la investigación no abarca un análisis detallado de las acciones realizadas. Con esta conclusión se pretende abrir una reflexión frente a las acciones y el comportamiento de Estados y empresas.

Un ejemplo importante de la instrumentalización del individuo para la securitización del ciberespacio es la situación actual protagonizada por China y Estados Unidos. Estos dos países se encuentran en una guerra comercial, debido a la cual los mandatarios de ambos países han obstaculizado la entrada de productos de su competidor a través de estrategias como el alza de impuestos y aranceles. Donald Trump firmó y presentó el 15 de mayo del 2019 una orden ejecutiva prohibiendo a las empresas estadounidenses utilizar los servicios de telecomunicaciones de cualquier firma extranjera "que ponga en riesgo la seguridad del país" y declaro un estado de emergencia, lo cual le permite al presidente tomar el control del comercio. Según el comunicado oficial de la Casa Blanca la orden se dio para "proteger a Estados Unidos de los adversarios extranjeros que están creando y explotando de forma activa y creciente vulnerabilidades en infraestructuras y servicios de tecnología de información y comunicación" (Trump, 2019).

La medida se tomó debido a las acusaciones a la empresa china Huawei de realizar actividades de espionaje a través de su tecnología y celulares. A pesar de la ausencia de pruebas públicas de prácticas maliciosas en los equipos de Huawei, la administración de Trump afirma que no se puede confiar en dichos productos porque Pekín puede intentar afectar los sistemas estadounidenses. Anteriormente se habían tomado medidas como la restricción de equipos Huawei y ZTE (otra empresa china) en sus bases militares y agencias federales.

Además, la empresa Huawei había sido acusada de actividades de vigilancia y espionaje por parte de otros países, a causa de esto Australia y Nueva Zelanda vetaron el uso de sus productos en las redes móviles de nueva generación 5G. Por su parte, Huawei niega que su trabajo conlleve ningún peligro de espionaje o sabotaje.

Sin embargo, la orden ejecutiva establecida por Trump tiene muchas más implicaciones de las esperadas. El 20 de mayo del presente año, Google comenzó a limitar los servicios de software que proporciona a Huawei, lo cual permite que los celulares funcionan y puedan descargar aplicaciones.

Sin embargo, debido a la censura y el control estricto que el gobierno ejerce en el ciberespacio chino, para los usuarios del país es normal tener un acceso restringido a Google

o YouTube. “La nueva postura agresiva de Estados Unidos simplemente acelerará ese proceso y abre la posibilidad de que un día los ciudadanos de China solo puedan usar celulares chinos y dispositivos impulsados por microprocesadores y programas creados en su país” (Yuan, 2019, párr. 6). Frente a las medidas Huawei respondió “Ni más seguro ni más poderoso. La decisión de EE.UU. les obligará a emplear equipos inferiores y costosos, quedándose atrás en el desarrollo de la tecnología 5G" (BBC Mundo, 2019, párr. 1). Lo que suceda en el contexto contemporáneo definirá el lugar del individuo y sus libertades en el ciberespacio y el modelo de gobernanza que se manejará internacionalmente.

Como reflexión personal es relevante agregar que el ciberespacio presenta una oportunidad muy grande para países como Colombia. La educación de alta calidad en el país es costosa y por lo tanto no está al alcance de una parte considerable del país. El internet es un elemento importante para la construcción de conocimiento en el país y también tiene un gran valor en la agencia del pueblo. Las noticias e información importante llegan a conocerse más a través de imágenes en redes sociales y cadenas de WhatsApp porque los medios oficiales solo cuentan una versión conveniente o no cuentan nada en lo absoluto. La privacidad en el ciberespacio ha sido un derecho claramente vulnerado por parte del gobierno hacía la población colombiana, las interceptaciones telefónicas y seguimientos ilegales realizados por la antigua agencia de inteligencia colombiana, el Departamento Administrativo de Seguridad es un claro ejemplo de esta situación (Caracol Radio, 2015).

El ciberespacio les da agencia a los individuos, actualmente es posible enterarse de los acontecimientos que suceden al otro lado del mundo debido al internet, es posible movilizar causas importantes y distribuir conocimiento. Más allá de eso, en el mundo globalizado se utiliza el internet constantemente para entablar relaciones con los demás, realizar transacciones, guardar información personal y mucho más. El gobierno y las empresas privadas deben garantizar el derecho a la privacidad e intimidad, y no utilizar a los individuos y su seguridad como pretexto para sus acciones, especialmente cuando estas terminan vulnerando los derechos de dichos individuos. Se espera que esta investigación contribuya a la reflexión frente a la gobernanza del ciberespacio y el respeto de los derechos individuales en este.

6. BIBLIOGRAFÍA

Alhindi, A., Talha, W., & Sulong, M. (2012). The Role of Modern Technology in Arab Spring. *Archives des sciences, 65*, 464-1661.

Barbe, É. (1987). El Papel Del Realismo En Las Relaciones Internacionales (La teoría de la política internacional de Hans J. Morgenthau). . *Revista de Estudios Políticos (Nueva Época), 57*.

Barbé, E. (2013). Narrativas del multilateralismo: «efecto Rashomon» y cambio de poder. *Revista CIDOB d'Afers Internacionals, 101*, 27-54.

BBC Mundo. (2014). *El FBI acusa al gobierno de Corea del Norte del hackeo a Sony Pictures.* . Obtenido de https://www.bbc.com/mundo/ultimas_noticias/2014/12/141219_ultnot_corea_norte

BBC Mundo. (2019). *Huawei: así respondió la tecnológica china a la decisión de Donald Trump de cerrarle la puerta del mercado de telecomunicaciones en EE.UU.* Obtenido de https://www.bbc.com/mundo/noticias-internacional-48295727

Caracol Radio. (2015). *Nuevas y escandalosas revelaciones sobre las 'chuzadas' del DAS.* Obtenido de Judicial: https://caracol.com.co/radio/2010/09/22/judicial/1285135320_361319.html

Cherepanov, A., & Lipovsky, R. (2016). *El troyano BlackEnergy ataca a una planta de energía eléctrica en Ucrania.* . Obtenido de We Live Security: https://www.welivesecurity.com/la-es/2016/01/05/troyano-blackenergy-ataca-planta-energia-electrica-ucrania/

El Tiempo. (2008). *Georgia acusa a Rusia de emprender una 'ciberguerra'*. Obtenido de Redacción Tecnología: https://www.eltiempo.com/archivo/documento/CMS-4442297

Gazapo, M. (2017). *Rusia, el Ciberespacio y las Elecciones estadounidenses.* . Obtenido de Comentario UNISCI. Vol 110.: https://www.ucm.es/data/cont/media/www/pag-72408//110MGAZAPO.pdf

Hoffman, S. (1990). A New World Order and Its Troubles. *Foreign Affairs, 19(4)*, 115-122.

Homeland Security. (2002). *Creation of the Department of Homeland Security.* Obtenido de https://www.dhs.gov/creation-department-homeland-security

Jinping, X. (2015). *Conferencia mundial de Internet.* Wuzhen: s/e.

Katzman, K. (2019). *Iran Sanctions.* Obtenido de Congressional Research Service: https://fas.org/sgp/crs/mideast/RS20871.pdf

Klingova, K. (2013). *Securitization of Cyber Space in the United States of America, the Russian Federation and Estonia.* Obtenido de Central European University Deparment of Political Science: http://www.etd.ceu.hu/2013/klingova_katarina.pdf

McGuinness, D. (2017). *Cómo uno de los primeros ciberataques de origen ruso de la historia transformó a un país.* Obtenido de BBC News: https://www.bbc.com/mundo/noticias-39800133

Muñoz, O., & Frasson, F. (2011). El realismo en el siglo XX y XXI. *Revista Analectas política, 1(1),* 81-106}.

Nojeim, G. (2010). *Cybersecurity and Freedom on the Internet.* Obtenido de Journal of National Security Law & Policy : http://jnslp.com/wp-content/uploads/2010/08/09_Nojeim.pdf

Obama, B. (2009). *Discurso enunciado el 29 de mayo de 2009 en la Casa Blanca.* Washington: White House.

Obama, B. (2009). *Text: Obama's Remarks on Cyber-Security.* Obtenido de The New York Times: https://www.nytimes.com/2009/05/29/us/politics/29obama.text.html

Orozco, S. (2013). Actores, estructura y proceso del orden político internacional contemporáneo. *Analecta Política, 4(6),* 99-120.

Prakash, D., & Klotz, A. (2008). *Qualitative Methods in International Relations: A Pluralist Guide (ECPR Research Methods)* . Reino Unido: Palgrave Macmillan.

Putin, V. (2018). *Sesión plenaria del Congreso Internacional de Ciberseguridad organizado por Sberbank, Data Economy y la Asociación de Bancos de Rusia.* Moscú: s/e.

Rennack, D., & Welt, C. (2019). *U.S. Sanctions on Russia: An Overview.* . Obtenido de Congressional Research Service. : https://fas.org/sgp/crs/row/IF10779.pdf

Schwartz, K. (2016). *The securitization of cyberspace through technifications.* Obtenido de [Thesis submitted to the faculty of the Virginia Polytechnic Institute and State University in partial fulfillment of the requirements for the degree of Master of Arts in Political Science]: https://vtechworks.lib.vt.edu/bitstream/handle/10919/71758/Schwarz_KJ_T_2016.pdf?sequence=1

Smith, M., Seifert, J., McLoughlin, G., & Dimitri, J. (2002). *The Internet and the USA PATRIOT Act: Potential Implications for Electronic Privacy, Security, Commerce, and Government. CRS Report for Congress.* . Obtenido de CRS Report for Congress: https://epic.org/privacy/terrorism/usapatriot/RL31289.pdf

Sputnik. (2016). *El número de usuarios de internet en China supera los 800 millones.* Obtenido de https://mundo.sputniknews.com/asia/201808221081386841-cuantos-chinos-utilizan-internet/

The White House. (2015). *Memorandum for heads of executive departments and agencies.* Obtenido de Executive Office of the president: https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2016/m-16-04.pdf

The White House. (2016). *Executive Order -- Establishment of the Federal Privacy Council.* Obtenido de https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/executive-order-establishment-federal-privacy-council

The White House. (2018). National Cyber Strategy of the United States of America. Donald J. Trump. Washington. D. C, EE.UU.

Treviño, J. (2016). ¿De qué hablamos cuando hablamos de la "securitización" de la migración internacional en México?: una crítica. *Foro Internacional 224 (2)*, 253-291.

Trump, D. (2019). *Comunicado de la Casa Blanca.* Washington: s/e.

Weaver, O. (1995). Chapter 3: Securitization and desecuritization. En R. Lipschutz, *On Securitty* (págs. 46-86,). s/e. Obtenido de https://www.libraryofsocialscience.com/assets/pdf/Waever-Securitization.pdf

Yuan, L. (2019). *Muro digital: las implicaciones de las sanciones estadounidenses a Huawei.* Obtenido de The New York Times: https://www.nytimes.com/es/2019/05/22/huawei-google-android/

Zeng, J., Stevens, T., & Chen, Y. (2017). China's solution to global cyber governance: Unpacking the domestic discourse of 'Internet sovereignty. *Politics & Policy 45(3)*, 432-464.

Zezima, K. (2015). *Obama signs executive order on sharing cybersecurity threat information.* Obtenido de The Washington Post: https://www.washingtonpost.com/news/post-politics/wp/2015/02/12/obama-to-sign-executive-order-on-cybersecurity-threats/?utm_term=.486ad2207524