PONTIFICIA UNIVERSIDAD CATOLICA DEL ECUADOR
FACULTAD DE COMUNICACIÓN, LINGÜÍSTICA Y LITERATURA
ESCUELA MULTILINGUE DE NEGOCIOS Y RELACIONES INTERNACIONALES

DISERTACIÓN DE GRADO PREVIA A LA OBTENCIÓN DEL TITULO DE LICENCIADA MULTILINGUE EN NEGOCIOS Y RELACIONES INTERNACIONALES

ANÁLISIS DE LOS EFECTOS EN LA HEGEMONÍA ESTADOUNIDENSE A CAUSA DE LAS AMENAZAS CIBERNÉTICAS Y LAS FALLAS DE SEGURIDAD PRESENTES EN SU SISTEMA DE CIBERDEFENSA. CASO SNOWDEN Y LA RESPUESTA DEL MANDATO DE BARACK OBAMA 2013 - 2016

ANDREA CAMILA FUENTES GUERRERO

JUNIO, 2018
QUITO – ECUADOR

AGRADECIMIENTO

A mis padres: Roberto y Marta, *gracias por todo su apoyo y el esfuerzo que han hecho para que pudiera tener la mejor educación. Gracias por ser mi guía y enseñarme la importancia del amor y la familia. Siento un orgullo inmenso de ser su hija. Los amo*

A mi tía Rosita, *no puedo expresar toda la gratitud que tengo contigo por siempre apoyar mis estudios e incentivarme a soñar en grande. También por enseñarme que el trabajo duro y honesto siempre será recompensado. Gracias tía.*

A mi ángel guardián: Cata *que a pesar de que te fuiste muy rápido siempre estás conmigo dentro de mi corazón. Te extraño tanto y aún me hacen falta tus consejos, tus besos y las películas que compartimos juntas en los momentos más difíciles. Gracias por ser una tía tan amorosa, que siempre supo dar lo mejor de sí.*

A mi mejor amiga: Marce, *decirte gracias es poco por todos los momentos que compartimos en la universidad. Siempre supiste darme un buen consejo cuando lo necesité y decirme la verdad por más dura que fuera. Gracias por cada locura, paseo, risas, aguacates, limas y tostado que compartimos. Gracias también por enseñarme que la vida siempre es mejor con un postre después del almuerzo. Te quiero muchísimo gordi y te extraño.*

A mi compañera de locuras: Vane López, *no he conocido mujer más loca y ocurrida en este mundo, gracias por los viernes de sushi después de italiano y tu amistad tan pura y divertida. Eres una de las pocas personas con las que puedo pasar años incomunicada y que con una llamada todo vuelve a la normalidad, como que no hubiera pasado un solo día. Prometo seguir rompiendo tus cigarrillos hasta que dejes de fumar. Te quiero amiga!*

A las amigas más increíbles que he conocido: Titina, Xime, Emi, Vane y Mafersita, *mis niñas hermosas, gracias por hacer de estos cuatro años de universidad los mejores de mi vida. Las peleas por el UNO, la organización del MunLEAI, las tardes de estudio, las fiestas, las donas y todo lo que comí con ustedes; pero sobre todo por ser esa luz que ilumina mi camino. Gracias por apoyarme en los mejores y peores momentos de mi vida, por abrir mi mente y hacer que entienda que las mujeres somos seres increíbles que podemos lograr todo lo que nos propongamos. Las amo y estoy sumamente orgullosa de ustedes.*

A mis primas: Emi y Sofi*, gracias por ser más que mis primas, mis hermanas. Sofi, aprendí tanto de ti, desde esa perseverancia para conseguir lo que quieres, hasta el saber aprovechar los momentos y el ojo que tienes para percibir las oportunidades que te presenta la vida. Emi, gracias por la confianza que tienes en mí, por ser la que me entiende en los momentos más raros de mi vida y por compartir mi amor por la música.*

A mi directora de tesis: Paola Lozada, *gracias por ayudarme y ser mi guía durante este proceso arduo de mi tesis, y sobre todo por ser del tipo de profesoras que inspiran a dar lo mejor y te incitan a pensar de manera crítica y no conformarse con respuestas simples.*
A mis profesores de LEAI, *de los cuales aprendí que el mundo iba mucho más allá de mi pequeña burbuja.*

ÍNDICE GENERAL

I. TEMA 1
II. RESUMEN 1
III. ABSTRACT 2
IV. RIASUNTO 2
V. GLOSARIO 4
VI. INTRODUCCIÓN 6

CAPÍTULO I
SMART POWER EN LA INTERDEPENDENCIA COMPLEJA 10

1.1. La interdependencia compleja 10
1.1.1. Política exterior: los cambios en la estructura 10
1.1.2. Características principales: Canales, agenda y fuerza militar 13
1.1.3. La evolución del poder desde el realismo a la interdependencia compleja 15
1.2. Distribución del poder: Estados, instituciones e individuos en la Política Mundial 18
1.2.1. El rol de Estado eclipsado por las instituciones 19
1.2.2. El ciberespacio: el poder de difusión de la información 23
1.2.3. Los recursos de poder en el ciberespacio 27
1.3. *Smart power*: aplicación de la inteligencia contextual 30
1.3.1. Aplicación del *smart power* a la política exterior 31
1.3.2. Características del *smart power*: armando la estrategia 35
1.3.3. Críticas de la teoría: ¿realmente funciona? 40

CAPÍTULO II
FILTRACIONES DE LA NSA: REPERCUSIONES EN LA POLÍTICA EXTERIOR CIBERNÉTICA ESTADOUNIDENSE 43

2.1. Antecedentes: filtraciones de WikiLeaks y medidas de defensa 43
2.1.1. Gobierno de Obama: el fortalecimiento de la ciberdefensa 44
2.1.2. WikiLeaks, las filtraciones de información clasificada 46
2.1.3. Las repercusiones para Estados Unidos y su respuesta 48
2.2. Caso Snowden: nuevas filtraciones de la Agencia Nacional de Seguridad (NSA) 54
2.2.1. Documentos clasificados filtrados de la Agencia Nacional de Seguridad 55
2.2.2. Marco Jurídico de la NSA y la legislación internacional pertinente al caso Snowden 59
2.2.3. Las violaciones al marco jurídico que rige la vigilancia masiva 63
2.3. Las repercusiones de las filtraciones en la política de ciberdefensa 65
2.3.1. La opinión pública nacional e internacional sobre las violaciones de privacidad 66
2.3.2. Reformulación legal: Ley de Ciberseguridad 72
2.3.3. Reestructuración de la Agencia Nacional de Seguridad 74

CAPITULO III
HEGEMONÍA DE ESTADOS UNIDOS FRENTE A ACTORES NO ESTATALES EN EL SISTEMA INTERNACIONAL 78

3.1. El poder de Estados Unidos versus Snowden en el quinto dominio 78
3.1.1. Capacidades y recursos de Estados Unidos en el ciberespacio 79
3.1.2. La agencia Nacional de Seguridad: las estrategias de las instituciones ...84
3.1.3. Analizando a Snowden: el ciberpoder de los actores no estatales 86
3.2. Análisis de la política exterior de ciberdefensa y la aplicación del *smart power* 90
3.2.1. El desafío de la Política Exterior estadounidense: "Estrategia para Actuar en el Ciberespacio" 2011 91
3.2.2. Ley del Ciberespacio 2015 y marco jurídico como fuente de poder 94
3.2.3. El *smart power*: ¿existe un balance de *soft* y *hard power* en la política exterior y las acciones de Estados Unidos? 97
3.3. La legitimación de la hegemonía estadounidense 98
3.3.1. Ciberguerra: la legitimación del uso del *hard power* 99
3.3.2. La hegemonía de Estados Unidos post-Snowden 102
3.3.3. Las razones de Snowden: ¿los actores no estatales representan una amenaza? 104

VII. CONCLUSIONES 108
VIII. RECOMENDACIONES 112
IX. LISTA DE REFERENCIAS 114

ÍNDICE DE TABLAS, CUADROS Y GRÁFICOS

TABLA 1
RECAPITULACIÓN: ACTOR Y SU RECURSO DE PODER EN EL CIBERESPACIO 29
TABLA 2
RECAPITULACIÓN: *SOFT POWER* Y *HARD POWER* EN LA ESTRATEGIA DEL *SMART POWER* 32
GRÁFICO 1
COMPARACIÓN PRESUPUESTOS DE DEFENSA ENTRE 2013 - 2016 34
GRÁFICO 2
COMPARACIÓN PORCENTAJES DE LAS ECONOMÍAS MUNDIALES ...35
IMAGEN 1
DETALLES RECOLECCIÓN DE DATOS *PRISM* 57
GRÁFICO 3
PORCENTAJE DE ACEPTACIÓN DE LOS PROGRAMAS DE VIGILANCIA 67
GRÁFICO 4
PORCENTAJE DE APROBACIÓN NACIONAL FRENTE A LOS PROGRAMAS DE VIGILANCIA 68
GRÁFICO 5

PORCENTAJE DE ACEPTACIÓN DE LO PROGRAMAS DE LA NSA Y POPULARIDAD DE ESTADOS UNIDOS....69
GRÁFICO 6
PORCENTAJE INTERNACIONAL DE CONFIANZA EN OBAMA....70
GRÁFICO 7
CONFIANZA EN LA PROTECCIÓN DE LAS LIBERTADES PERSONALES EN LOS ESTADOS UNIDOS....71
IMAGEN 2
RECOLECCIÓN DE DATOS DEL CENTRO DE UTAH....76
GRÁFICO 8
MERCADO GLOBAL DE SISTEMAS OPERATIVOS 2013 – 2017....81
GRÁFICO 9
MERCADO GLOBAL DE MOTORES DE BÚSQUEDA 2010 – 2017....82
GRÁFICO 10
MERCADO GLOBAL DE PROVEEDORES DE SERVICIOS DE ALMACENAMIENTO DIGITAL 2016....83
GRÁFICO 11
MAYORES PROBLEMAS DE SEGURIDAD CIBERNÉTICA EN ESTADOS UNIDOS HASTA 2016....101
GRÁFICO 12
INDUSTRIAS MÁS ATACADAS POR EL CIBERESPIONAJE 2016....102

ÍNDICE DE ANEXOS

ANEXO 1
U.K. – U.S. COMMUNICATIONS INTELLIGENCE AGREEMENT (UKUSA AGREEMENT)....125

I. TEMA

ANÁLISIS DE LOS EFECTOS EN LA HEGEMONÍA ESTADOUNIDENSE A CAUSA DE LAS AMENAZAS CIBERNÉTICAS Y LAS FALLAS DE SEGURIDAD PRESENTES EN SU SISTEMA DE CIBERDEFENSA. CASO SNOWDEN Y LA RESPUESTA DEL MANDATO DE BARACK OBAMA 2013 – 2016

II. RESUMEN

La globalización es un proceso que revolucionó el mundo en aspectos económicos, sociales, culturales y políticos, creando la interdependencia entre los distintos actores del sistema internacional. Este fenómeno cambió la concepción del mundo, basado en la dicotomía de Realismo – Idealismo, de tal manera que se establece un modelo capaz de incorporar nuevos actores y contextos. El ciberespacio, instituciones e individuos se han visto como amenazas a la legitimación del poder de los Estados, que encuentran un escenario invadido por los intereses de estos nuevos actores, que atentan con eclipsar su accionar. En 2013, la filtración de información confidencial de los programas de vigilancia mundial de la Agencia Nacional de Seguridad de Estados Unidos (NSA) por parte de Edward Snowden expuso varias violaciones a los derechos civiles y constitucionales con el objetivo de espiar a posibles criminales. No obstante, las publicaciones revelaron fines políticos encubiertos bajo la campaña "Guerra Contra el Terrorismo". La presente investigación concluyó que el poder de Estados Unidos después de las filtraciones, se ve eclipsado por los nuevos actores y sus intereses dentro del ciberespacio. Sin embargo, la influencia mundial que tiene el mismo en el sistema internacional no sufre cambios significativos. El marco metodológico utilizado fue una investigación cualitativa que analiza la política exterior de los Estados Unidos a través de sus estrategias, leyes y discursos referentes a la ciberdefensa. Además, se utilizaron elementos de investigación cuantitativa, como estadísticas y presupuestos, para respaldar la tesis principal.

Palabras clave: ciberespacio, información clasificada, Agencia Nacional de Seguridad, Estados Unidos, Edward Snowden

III. ABSTRACT

Globalization is a process that revolutionized the world in economic, social, cultural and political aspects, creating interdependence among the different actors of the international system. This phenomenon changed the conception of the world, based on the dichotomy of Realism - Idealism, in such way that a model capable of incorporating new actors and contexts is established. Cyberspace, institutions and individuals represent threats to the legitimation of the power of States. They find a scenario invaded by the interests of these new actors, which attempt to eclipse their actions. In 2013, the leaks of confidential information from the United States National Security Agency's (NSA) global surveillance programs by Edward Snowden exposed several violations of civil and constitutional rights with the aim of spying on potential criminals. Nevertheless, the publications revealed covert political ends under the "War on Terrorism" campaign. The present investigation concluded that US power after new actors and their interests within cyberspace overshadow the leaks. However, the global influence it has in the international system did not undergo significant changes. The methodological framework used for this investigation was a qualitative research that analyzes US foreign policy through its strategies, laws and speeches referring to cyber defense. In addition, elements of quantitative research such as statistics and budgets were used to support the main thesis.

Keywords: cyberspace classified information, National Security Agency, United States, Edward Snowden

IV. RIASUNTO

La globalizzazione è un processo che ha rivoluzionato il mondo in termini economici, sociali, culturali e politici, creando interdipendenza tra i diversi attori del sistema internazionale. Questo fenomeno ha cambiato la concezione del mondo, sulla base della dicotomia del Realismo - Idealismo, in modo tale da stabilire un modello capace di incorporare nuovi attori e contesti. Il cyberspazio, le istituzioni e gli individui rappresentano minacce alla legittimazione del potere degli Stati, chi trovano uno scenario invaso dagli interessi di questi nuovi attori,

che tentano di eclissare le loro azioni. Nel 2013, la filtrazione di informazioni riservate dai programmi di sorveglianza globale dell'Agenzia per la Sicurezza Nazionale degli Stati Uniti (NSA) di Edward Snowden hanno esposto diverse violazioni dei diritti civili e costituzionali allo scopo di spiare potenziali criminali. Tuttavia, le pubblicazioni hanno rivelato finalità politiche segrete nell'ambito della campagna "Guerra al terrorismo". La presente inchiesta ha concluso che il potere degli Stati Uniti dopo le falle è messo in ombra dai nuovi attori e dai loro interessi all'interno del cyberspazio. Nonostante, l'influenza globale che ha nel sistema internazionale non ha sofferto cambiamenti significativi. Il quadro metodologico utilizzato per questa indagine è stata una ricerca qualitativa che analizza la politica estera degli Stati Uniti attraverso le sue strategie, leggi e discorsi relativi alla difesa cibernetica. Inoltre, elementi di ricerca quantitativa come statistiche e budget sono stati utilizzati per supportare la tesi principale.

Parole chiave: cyberspazio informazione classificata, Agenzia Nazionale per la Sicurezza, Stati Uniti, Edward Snowden

V. GLOSARIO

Cable diplomático – El cable diplomático, también conocido como telegrama diplomático o cable de la embajada, es un mensaje de texto confidencial intercambiado entre una misión diplomática, como una embajada o un consulado, y el Ministerio de Relaciones Exteriores de su país de origen (The Macquarie Dictionary*)*.

Ciberespacio – Red interdependiente de infraestructuras de tecnología de la información que incluye Internet, redes de telecomunicaciones, computadoras, sistemas de información o comunicaciones, redes y procesadores y controladores integrados. (Fuente: Política de Operaciones Cibernéticas de Estados Unidos, 2008)

Ciberinteligencia – La recopilación, procesamiento, análisis y difusión de información de todas las fuentes de inteligencia sobre los programas cibernéticos, intenciones, capacidades, investigación y desarrollo, tácticas y actividades e indicadores operacionales de los actores extranjeros; Su impacto o efectos potenciales sobre la seguridad nacional, los sistemas de información, la infraestructura y los datos; Y la comprensión de los componentes, estructuras, uso y vulnerabilidades de los sistemas de información extranjeros. (Oficina del Director de Inteligencia Nacional, Estrategia de Inteligencia Nacional 2014)

Ciberdefensa - Una medida proactiva para detectar u obtener información sobre una intrusión cibernética, un ataque cibernético o una operación cibernética inminente o para determinar el origen de una operación que implica el lanzamiento de una contra-operación preventiva o cibernética contra la fuente (Open Technology Institute New America, 2013).

Ciberseguridad – La prevención del daño, el uso no autorizado o la explotación y, en caso necesario, la restauración de los sistemas electrónicos de información y comunicaciones y la información contenida en ellos para garantizar la confidencialidad, integridad y disponibilidad; Incluye la protección y la restauración, cuando sea necesario, de redes de información, sistemas de comunicaciones y sistemas de control inalámbricos, por satélite, de seguridad pública y 911 (Departamento de Seguridad Nacional de los Estados Unidos, Plan Nacional de Protección de la Infraestructura, 2013).

Ciberamenaza – Una circunstancia o evento que tiene o indica el potencial para explotar las vulnerabilidades y afectar adversamente las operaciones organizacionales, los activos de la organización (incluidos los sistemas de información e información), los individuos, otras organizaciones o la sociedad. (Departamento de Seguridad Nacional, Iniciativa Nacional para la Seguridad Cibernética Carreras y Estudios)

Ciberterrorismo – El Centro de Estudios Estratégicos e Internacionales (CSIS) lo define como "el uso de herramientas informáticas para interceptar

infraestructuras nacionales críticas (energía, transporte, operaciones gubernamentales), coaccionar o intimidar a un gobierno o a una población civil.

Ciberactivismo – El uso de correo electrónico, blogs y sitios de redes sociales para dar a conocer una causa mediante la difusión de información que no está disponible a través de las fuentes normales de noticias gubernamentales y comerciales, que pueden o no alcanzar eventualmente.

Información clasificada – La información clasificada de seguridad nacional es información creada o recibida por una agencia del gobierno federal o un contratista gubernamental que dañaría la seguridad nacional si fuera liberada indebidamente. La información clasificada puede tomar cualquier forma. Aunque los documentos en papel son los más comunes, hay fotografías clasificadas, mapas, películas, videos, bases de datos, microfilmes, discos duros, CDs, etc. Independientemente del medio, la información clasificada requiere protección hasta que sea formalmente desclasificada.

- "Top secret" daño excepcionalmente grave a la seguridad
- "Secret" información cuya liberación causaría "daño grave"
- "Confidential" es la categoría más baja de información clasificada actualmente en uso.

Inteligencia contextual - La habilidad diagnóstica intuitiva que ayuda a los políticos a alinear las tácticas con objetivos para crear estrategias inteligentes (Nye, 2009)

Nación digital – El uso del internet de alta velocidad en las operaciones diarias de una nación, es decir en la parte económica, política, académica y social. Potenciar el desarrollo de la industria tecnológica en base a la demanda del servicio, incrementando los niveles de adaptabilidad y seguridad (NTIA, 2013).

VI. INTRODUCCIÓN

El fin de la Guerra Fría transformó la dinámica de poder en el escenario internacional debido a la globalización y el desarrollo de la tecnología. Estos fenómenos descentralizaron el poder en diferentes contextos y actores. Instituciones, empresas e incluso individuos surgieron como actores claves dentro de la toma de decisiones, influyendo en la política mundial. Nye (2010) establece que la creación del ciberespacio fue un hito dentro de la concepción y la naturaleza del poder, pues se convierte en un nuevo dominio, con nuevas reglas que mutan constantemente. El ciberespacio además crea nuevas oportunidades, así como amenazas para las cuales los Estados no se encuentran preparados. Por lo tanto, la seguridad es una nueva forma de poder, en especial en cuanto a información se refiere. Se vive en una época, en la cual la información constituye una fuente de poder sin precedentes, y el internet, el nuevo medio de comunicación, se convierte en el principal difusor y almacenador de la misma.

El internet ofrece libre acceso y barreras de entrada muy bajas que permiten que cualquier actor lo use, incluso gozando de anonimato durante su permanencia. Existe una regulación por parte de organizaciones internacionales que establecen principios generales que delinean sus operaciones y la manera en que estas llegan al público. Sin embargo, estas organizaciones no logran crear acuerdos globales y dado que el internet no posee una nacionalidad concreta ni soberanía propia, ningún Estado puede normar su uso específico sin coartar las libertades de otros Estados y sus ciudadanos. A pesar de la existencia de dichas leyes que regulan y sancionan actividades como el espionaje, ataques cibernéticos, violación de privacidad, etc., la mutabilidad del ciberespacio no permite que la legislación se adapte acorde a los cambios acelerados de la tecnología. Además, el anonimato que brinda este dominio constituye una vulnerabilidad para los Estados, los cuales no poseen los recursos y capacidades necesarios para identificar a aquellos individuos que perpetran los cibercrímenes.

Teniendo en cuenta los puntos mencionados, el presente trabajo de investigación se plantea como objetivo general: identificar las repercusiones en el poder de un Estado cuando existen fallas de seguridad cibernéticas que dejan vulnerable la información de los gobiernos, tomando como caso las filtraciones de los documentos clasificados que Edward Snowden reveló al mundo. El caso expone que la política exterior estadounidense ha sido incapaz de adaptarse al cambio continuo de la tecnología, puesto que sus estrategias no han proporcionado los resultados esperados. A pesar que durante el discurso inaugural del mandato de Barack Obama se resaltó la importancia del manejo del ciberespacio como herramienta clave para el progreso del país, se puede inferir una subestimación del potencial y alcance que este puede tener. La política exterior de ciberdefensa exhibe un uso del ciberespacio como arma de ataque frente al terrorismo, sin embargo no es utilizado como una herramienta de defensa, dejando a los sistemas y redes desprotegidos del espionaje.

Snowden, más allá de exponer la violación a los derechos de privacidad que Estados Unidos lleva a cabo mediante sus programas de espionaje mundial, también demuestra que no tiene un sistema de contingencia frente a los mismos. Estados Unidos se dedicó a cazar al traidor que reveló sus secretos, sin darse cuenta que la verdadera lección que este individuo les dejó fue la del progreso. Snowden (2013) declaró: "Estoy dispuesto a sacrificar toda mi vida porque mi consciencia no me permitiría dejar que el gobierno de los Estados Unidos destruya nuestra privacidad, la libertad de internet y las libertades básicas de las personas alrededor del mundo con esta máquina masiva de vigilancia que están construyendo"[1] Sus motivaciones estaban dirigidas hacia la defensa de la transparencia, como él mismo declara: "Existen varios tipos de documentos que podrían haber creado gran impacto, pero que no entregué porque mi objetivo no es perjudicar a nadie. La transparencia sí."[2] Sus preocupaciones surgieron cuando los expertos de la Agencia Nacional de Seguridad (NSA) no lograron detectar las

[1] Snowden: "I'm willing to sacrifice all of that because I can't in good conscience allow the US government to destroy privacy, internet freedom and basic liberties for people around the world with this massive surveillance machine they're secretly building".
[2] "There are all sorts of documents that would have made a big impact that I didn't turn over, because harming people isn't my goal. Transparency is."

pistas virtuales que dejó en los documentos robados. Por lo tanto, instó a las autoridades a concentrar sus esfuerzos en la defensa de su información y mejorar los procesos de detección, en vez de enfocarse en expandir su poder mediante el espionaje.

La presente investigación contiene una estructura que enfatiza la importancia de la teoría; consecuentemente, su desarrollo está comprendido como una descripción de la misma, desde su desarrollo y contexto histórico, seguido por una explicación del caso escogido, y finalmente, realiza un análisis en conjunto. El primer capítulo pretende analizar el concepto de *smart power* en un sistema internacional anárquico donde el protagonismo de los Estados se ve afectado por individuos y actores externos. Esta teoría es creada por Joseph Nye a inicios de los años 2000 al entender que la aplicación del *hard power* o el *soft power* individualmente, no proporciona los resultados deseados. Sin embargo, aplicados en conjunto y teniendo en cuenta el contexto, ambos poderes crean una estrategia de política exterior que proporciona un enfoque holístico. Cabe recalcar que esta iniciativa surge bajo el marco de la Interdependencia Compleja, teoría de las relaciones internacionales creada por el mismo autor en conjunto con Robert Keohane. La teoría explica los cambios que surgen con la finalización de la Guerra Fría, por la cual en el sistema internacional surgen actores no estatales que alteran la toma de decisiones mediante la imposición de sus intereses. Además, se observa que la militarización de un Estado ya no logra controlar a otros actores y los temas de la agenda internacional varían según las necesidades de la población. Finalmente, se utiliza la teoría de la hegemonía, con la finalidad de demostrar el poder en su máxima potencia. Esta teoría es analizada por el mismo autor (Keohane) y bajo el marco de la interdependencia compleja.

El segundo capítulo busca determinar las repercusiones en la política de ciberdefensa de Estados Unidos como respuesta a las filtraciones de información clasificada por parte de Edward Snowden. Este capítulo describe la política exterior estadounidense y las medidas que el gobierno tuvo que tomar después de

las filtraciones. De la misma manera, se analiza la opinión pública mundial frente a los programas de espionaje y las repercusiones en la diplomacia.

Finalmente, el tercer capítulo se desarrolla con el análisis de la aplicación del *smart power* en el marco de la interdependencia compleja en el caso de Estados Unidos como actor estatal frente a Edward Snowden. Este capítulo analiza las repercusiones en la hegemonía estadounidense frente al contexto descrito por la teoría, para comprender los cambios suscitados en política exterior.

El trabajo de investigación plantea, en lugar de una hipótesis, una pregunta de investigación, la cual busca determinar si la hegemonía de Estados Unidos se ha visto afectada por las fallas de seguridad de la Agencia Nacional de Seguridad, las cuales fueron expuestas cuando Edward Snowden filtró la información clasificada con respecto a la política exterior del gobierno de Obama. Por consiguiente, la disertación se desarrolló bajo la metodología cualitativa mediante el estudio de los documentos oficiales de gobierno, discursos presidenciales, tratados, informes y estrategias que precisan la descripción del caso y la evaluación de sus repercusiones. Sin embargo, para apoyar los resultados encontrados en el análisis, se utilizaron herramientas de la metodología cuantitativa mediante el estudio de estadísticas.

La investigación corresponde al perfil del área de las Relaciones Internacionales de la carrera Multilingüe en Negocios y Relaciones Internacionales, puesto que aplica un enfoque multidisciplinario del caso al tomar elementos de política exterior, derecho y cooperación internacional. Así también, dentro del ámbito de los negocios se puede analizar el ciberespacio como herramienta para el progreso económico de un país y las estrategias utilizadas para impulsar este sector. Esta investigación contribuye en un ámbito internacional dado que la regulación del ciberespacio es un tema que concierne a todos los Estados y, que a través del estudio de este se podría evitar una tercera guerra mundial manejada desde este nuevo dominio.

CAPÍTULO I

SMART POWER EN LA INTERDEPENDENCIA COMPLEJA

1.4. La interdependencia compleja

La interdependencia compleja es una teoría de las Relaciones Internacionales que critica los supuestos principales del realismo. Fue creada por Robert Keohane y Joseph Nye a finales de 1970 y es presentada en su libro "Poder e Interdependencia". Los autores desarrollan esta teoría en vista de los cambios presentes en el sistema internacional al finalizar la Guerra Fría, y aseguran que sus supuestos se aproximan de manera más certera al contexto internacional, puesto que el realismo no toma en cuenta ciertos aspectos necesarios para el desarrollo de las relaciones internacionales (Keohane & Nye, 1977).

La interdependencia compleja hace referencia a las tres características principales presentes en la nueva era. Los canales múltiples, ausencia de jerarquía y la reducción de la fuerza militar; de la misma manera realiza un análisis del poder en el sistema internacional como instrumento de la política. La importancia de esta teoría reside en la inclusión de nuevos actores que son una parte fundamental en la explicación del nuevo contexto, pues tienen la capacidad de modificar el proceso de toma de decisiones para lograr imponer sus intereses en la formulación de políticas (Keohane & Nye, 1977).

A continuación, se expondrán los principios de la teoría de la Interdependencia Compleja en la política exterior, mediante la descripción de su evolución; seguido de la explicación de sus características y la manera en la que modifica el poder y su uso en las Relaciones Internacionales.

1.4.1. Política exterior: los cambios en la estructura

La interdependencia ha cambiado la política mundial debido a que surgen nuevas amenazas y posibilidades para los actores. Los problemas y sus soluciones son más complejos por cuanto cada decisión afecta a otros sectores e incluso a otros actores. Los temas sociales, ecológicos y económicos son una parte

fundamental de la política, pues los intercambios y las telecomunicaciones han acercado al mundo, tornando ciertas amenazas en asuntos mundiales (Keohane & Nye, 1977). Lester R. Brown asegura que gracias a este fenómeno de la interdependencia el mundo deja de tener fronteras, convirtiéndolo en una aldea global (Brown, 1972). Otro fenómeno que puede observarse, es el surgimiento de nuevos actores, que eclipsan el accionar de los Estados. Las corporaciones multinacionales y transnacionales, así como las organizaciones internacionales cobran importancia y modifican los procesos de toma de decisiones al imponer sus intereses (Keohane & Nye, 1977).

Desde la década de los 60, se empiezan a notar los cambios en el sistema internacional, por el hecho que la seguridad y la fuerza militar dejaban de ser el centro de las problemáticas mundiales; lo que no quiere decir que sean irrelevantes, sino que aparecieron diferentes temáticas que requerían de la atención de los actores. Keohane y Nye (1977) aseguran que "en política mundial, interdependencia se refiere a situaciones caracterizadas por efectos recíprocos entre países o entre actores en diferentes países" (pág.22). Dichos efectos se derivan de los intercambios internacionales que se intensifican después de la segunda guerra mundial, refiriéndose más a las limitaciones y costos que impliquen dichos intercambios, pues cuando no existen efectos de costo relevantes solo se puede hablar de interconexión. Los efectos de costo son impuestos directa e intencionalmente por los actores cuando existe una amenaza, cualquier sea su naturaleza, que emane de uno de ellos o de ambos. Por otro lado, existe interdependencia debido a la cooperación entre Estados o actores por una amenaza externa (Keohane & Nye, 1977).

La relación entre los actores está caracterizada por la cooperación y la competencia. Basados en este sistema los actores cooperan debido a intereses comunes para lograr la prosperidad y estabilidad en el sistema internacional (Rana, 2015). Después de la Segunda Guerra Mundial, la cooperación internacional y el apoyo a Naciones Unidas tomaron fuerza, así del mismo modo las alianzas y la asistencia externa; sentimiento que acrecentó durante la Guerra

Fría a la par de la seguridad nacional y las intervenciones militares. Pero de la misma forma que se resaltaron los conceptos realistas, hacia la finalización de la guerra, el término "seguridad nacional" perdió fundamento y, por lo tanto el intervencionismo militar (Keohane & Nye, 1977).

Es así que, finalizada la Guerra, la política mundial cambia radicalmente, la seguridad deja de ser el principal problema para los Estados y la fuerza militar pierde valor, y por lo tanto el poder que este asignaba a los mismos. Al considerar esto, es necesario entender que no existe un poder único, sino distintas gamas del mismo; por esta razón la interdependencia genera nuevas formas de conflicto y puede llegar a acrecentar los mismos. De esta manera las relaciones interdependientes se pueden analizar desde dos perspectivas diferentes, donde la primera se refiere a las ganancias o pérdidas comunes de los actores; mientras que la otra hace referencia a las ganancias relativas y la distribución de las mismas. La interdependencia toma en cuenta esta distribución como un punto importante dentro del análisis de la política mundial (Keohane & Nye, 1977).

La distribución desigual de las ganancias se da debido a las asimetrías presentes en los actores. Aquellos actores que sean menos dependientes, usarán esta capacidad como fuente de poder; mientras que los que sean más dependientes tendrán ganancias menores frente a otros actores. Como resultado, se requiere enfatizar que los intereses realistas han quedado atrás, por lo que el uso de la fuerza militar de desvaloriza y se toma en cuenta la distribución de los recursos de poder en los diversos temas de la agenda. Otro tema a tomar en cuenta es el surgimiento de nuevos actores no estatales que limitan el accionar de los Estados y los obligan a actuar basados en sus intereses. De la distribución del poder también se explica el hecho que Estados pobres y débiles empleen la asimetría como fuente de poder, así como usar a los actores no estatales en su beneficio (Keohane & Nye, 1977).

1.4.2. Características principales: Canales, agenda y fuerza militar

La teoría de la interdependencia compleja surge en vista de los cambios presentes en el sistema internacional posguerra, ya que aseguran que el realismo no toma en cuenta varios aspectos fundamentales presentes en la política mundial. Cabe aclarar que el realismo parte de tres supuestos principales, el primero determina a los Estados como unidades coherentes protagonistas de la política mundial; en segundo lugar, establece que la fuerza o coerción es una herramienta válida en la política, lo que termina por fijar la agenda de manera jerárquica donde la seguridad militar predomina por sobre los temas económicos y sociales (Keohane & Nye, 1977).

Por el contrario, la interdependencia compleja establece tres características principales: canales múltiples, ausencia de jerarquía de la agenda y menor militarización. La primera característica hace referencia a las relaciones entre los actores, estas pueden ser de carácter interestatal, transgubernamental y transnacional. En segunda instancia, la ausencia de jerarquía en la agenda estipula que la seguridad militar ya no es el principal interés de un Estado. Finalmente, el menor papel de la fuerza militar está relacionado directamente al segundo principio. Si existen diversos temas prioritarios en la agenda, no todos pueden ser resueltos mediante la fuerza (Keohane & Nye, 1977).

Canales múltiples

La globalización ha provocado un acercamiento entre las naciones y actores no gubernamentales debido al desarrollo de la tecnología; por lo tanto la comunicación juega un papel importante en las relaciones internacionales. Existen los nexos informales entre élites gubernamentales donde se dan acuerdos formales; de la misma manera se dan nexos entre élites no gubernamentales y organizaciones transnacionales. Estas comunicaciones se denominan como relaciones interestatales, transgubernamentales y transnacionales, lo cual amplía las posibilidades, que según los realistas las relaciones interestatales son las únicas que son válidas. La interdependencia admite nuevos actores que puede modificar

la política mundial, dado que influyen en economía, problemas sociales y ecológicos (Keohane & Nye, 1977).

Un ejemplo claro del cambio que presentan los nuevos actores son las empresas y bancos multinacionales, pues no solo inciden en las relaciones internas, pero también a nivel interestatal. La participación de estas instituciones no estatales se ha convertido en un elemento común dentro de la sociedad que ha creado nuevas problemáticas internas y, sobre todo externas que afectan la toma de decisiones; así mismo se pierde el límite entre lo interno y externo, por la afectación presente en las decisiones de ambos niveles. Esto significa que la formulación de políticas se convierte en un tema de análisis que no puede dejar de lado a otros actores (Keohane & Nye, 1977).

Ausencia de jerarquía

La seguridad militar ha quedado atrás como el principal tema de la agenda internacional, cabe recalcar que continúa siendo importante, pero la jerarquía presente en la política exterior ha quedado obsoleta. Cuestiones relevantes como los temas económicos, sociales y ecológicos han surgido debido a la aparición de actores no estatales que interponen sus intereses en la agenda (Keohane & Nye, 1977). En 1975, Henry Kissinger dijo "ha surgido una gama de cuestiones nuevas y sin precedentes" (pág. 199). Puso como ejemplo los acuerdos consultivos globales de las diferentes instituciones internacionales que demuestran el solapamiento de las cuestiones internas y externas en la formulación de políticas (Kissinger, 1975).

Varias de las nuevas problemáticas atentan contra grupos internos dificultando la tarea de la formulación de políticas coherentes y consistentes. A su vez, los cambios en las políticas externas significaban cambios en la política interna y viceversa. Los líderes de Estados alrededor del mundo entendieron que la aplicación de la fuerza no ayudaría a resolver los problemas, por lo que se vieron

obligados a buscar soluciones fuera de la seguridad militar (Keohane & Nye, 1977).

Reducción de la fuerza militar

Se debe tomar en cuenta que la seguridad ya no se resume a la supervivencia física, sino que también hace referencia a la económica, social, ecológica, etc. De la misma manera, al existir diversos actores, la dirección de donde proviene la amenaza es incierta y múltiple. La fuerza deja de ser un medio apropiado para satisfacer los intereses del Estado y en varias situaciones sus efectos resultan inciertos y costosos. Posterior a la guerra, los Estados en general buscan salvaguardar la paz, por lo tanto el uso de la fuerza atenta contra estos intereses, no solo mantener un estado de guerra constante resulta altamente costoso, sino también innecesario. Existen varios canales a ser utilizados como la diplomacia y la cooperación dejando que el uso de la fuerza se convierta en obsoleto frente a problemáticas económicas, sociales o ecológicas. No obstante, países como Estados Unidos, Rusia o China mantienen altos presupuestos destinados a la industria militar como medida de seguridad en posibles ataques o como una herramienta necesaria en conflictos armados que se desarrollan de tiempo en tiempo, y en los que es necesario el uso de la fuerza (Keohane & Nye, 1977).

1.4.3. La evolución del poder desde el realismo a la interdependencia compleja

El poder es un concepto necesario en la explicación de las relaciones internacionales, igualmente complejo. Dentro del realismo se analiza la lucha de poder dentro de la política internacional como uno de los ejes fundamentales de la teoría, pero debido a los cambios suscitados en el sistema, su concepción y uso varían, requiriendo un nuevo enfoque, en este caso la interdependencia compleja, que explique la influencia de dichos cambios. El poder es un elemento fundamental en la formulación de la política exterior, por lo que su análisis puntual esclarece los recursos disponibles, su uso y las posibilidades que estos ofrecen (Creus, 2013).

En 1948, Hans Morgenthau define al poder como "el control del hombre sobre las mentes y acciones de otros hombres" (pág. 51), para luego complementar con una definición de poder político que lo define como "una relación entre los que lo ejercen y aquellos sobre los cuales es ejercido" (pág. 215). Morgenthau, posteriormente, puso énfasis en la posesión de recursos como fuente de poder nacional, especialmente en las capacidades militares y económicas. También reconoce que la diplomacia es un elemento importante dentro del poder nacional, pero sugiere utilizarlo cautelosamente por la inestabilidad de su naturaleza (Creus, 2013).

Parte del neorrealismo, Kenneth Waltz, en su libro *Teoría de la Política Internacional* (1979), simplificó la definición de poder, regresando al realismo clásico, el cual está fundamentado en la posesión de recursos materiales sean militares y económicos, lo que lo convierte en algo medible y que puede ser acumulativo (Creus, 2013). De manera lógica se podría entender que más recursos un Estado posee, más poder tiene; pero la realidad es mucho más compleja que este supuesto. En este punto se debe diferenciar entre el poder potencial y el real, visto que un mal manejo de los recursos (potencial) puede concluir con una pérdida de poder, por lo tanto, un análisis que toma en cuenta variable y factores llega a comprender realmente la complejidad y la verdadera forma de obtener poder. La globalización es el punto de inflexión entre la concepción realista y la interdependiente (Creus, 2013).

Keohane y Nye, comprenden el cambio de la naturaleza del poder que se ve afectado por los avances tecnológicos, las comunicaciones y el surgimiento de nuevos actores (Creus, 2013). Nye (2009), describe al poder como la habilidad de afectar el comportamiento de otros para obtener lo que se desea. Considerando que existe una multiplicidad de actores que afectan directamente a las relaciones de poder y que los actores en el sistema internacional son asimétricos, es decir que no poseen las mismas capacidades, este fenómeno se convierte en una importante

fuente de poder estructural[3] (Arenal, 2009). Por lo tanto, es indispensable contextualizar la utilización del poder para la administración eficaz y eficiente de los recursos, tomando en cuenta las fortalezas y debilidades propias y ajenas (Creus, 2013).

En la interdependencia compleja se lo identifica bajo dos dimensiones centrales: la sensibilidad y vulnerabilidad. La primera se refiere al grado de respuesta en una estructura política, es decir la rapidez con la que los cambios en un país producen cambios en otro y qué tan costosos resultan los mismos. Esta supone que el marco permanecerá sin variaciones. Por otro lado, la vulnerabilidad se refiere a la disponibilidad relativa y los recursos empleados que deben asumir los actores debido a las acciones que toman para sopesar los cambios. En otras palabras, la sensibilidad es la contingencia que tiene un país frente a los cambios para que las políticas no sean modificadas, mientras que la vulnerabilidad representa una desventaja frente a los cambios a pesar de la modificación de sus políticas (Keohane & Nye, 1977).

En política, las relaciones entre actores constituyen un principio primordial donde el poder opera en tres dimensiones. La primera es la capacidad para dirigir los cambios a través del uso directo del poder de un actor sobre otro. La segunda dimensión hace referencia al control de la agenda para de esta manera restringir el accionar de otros actores, usando el poder de manera indirecta. Finalmente, se encamina a las preferencias y la manera de adaptarlas hacia los intereses propios (Nye, 2011). La concepción de la interdependencia se centra principalmente en la primera dimensión, pero su enfoque en las instituciones y la cooperación le permiten analizar de la misma manera la segunda dimensión (Creus, 2013).

Se debe agregar que existen diferentes maneras de alcanzar el poder. Mediante el *soft power* y el *hard power*, los cuales utilizan métodos contrapuestos para lograr obtener los resultados deseados. Nye (2011) define al *hard power*

[3] El control de los recursos y la capacidad de afectar o modificar el resultado final. (Keohane & Nye, 1977)

como la habilidad de conseguir que un actor alcance objetivos impuestos por otro, a pesar de que estos no están alineados con sus políticas, preferencias y estrategias lo cual se realiza mediante la imposición de la fuerza o amenazas. Por el contrario, el mismo autor define al *soft power* como la habilidad de conseguir que un actor logre ciertos objetivos que han sido impuestos por otro actor, pero que los asume como propios (Nye, 1990).

Las fuentes que el *hard power* utiliza son las amenazas y los incentivos mediante la intimidación, pagos y recompensas. El término es usado principalmente en el realismo, dado que según los teóricos pertenecientes a esta corriente, el uso de la fuerza y el poderío militar constituyen una herramienta principal para lograr el objetivo de seguridad nacional (Waltz, 1979). Keohane y Nye, se enfocan más en las soluciones diplomáticas, de no resolver los conflictos presentes se hará uso del *hard power* como el último recurso (Keohane & Nye, 1977) .

El *soft power*, por el contrario, utiliza la tracción y persuasión mediante el uso de las cualidades inherentes y la comunicación. Los elementos de este tipo de poder son la cultura, los valores y las políticas, y su importancia se resalta debido a que tiene una influencia mayor que el *hard power* pues toma en cuenta la diplomacia y la cooperación. Al trabajar en conjunto con otros países o actores se puede llegar a consensos y permite que los intereses de todos se encuentren propiamente representados. El *soft power* de esta manera se considera como una estrategia a largo plazo porque representa legitimidad, credibilidad y confianza (Nye, 2004).

1.5. Distribución del poder: Estados, instituciones e individuos en la Política Mundial

En la interdependencia la dinámica del poder se transforma, principalmente en el cambio de *hard power* a *soft power*; el nuevo sistema incita a la reducción del uso de la fuerza debido a los costos que este implica y dado que el poder ha evolucionado a múltiples dimensiones y distintos escenarios. En la

Interdependencia Compleja el poder es un recurso para alcanzar los objetivos propuestos por los actores, sin embargo no es posible su medición si no se tiene en cuenta el propósito de su uso (Keohane & Nye, 1977).

El poder se hace referencia al control que un actor tiene sobre otro para alcanzar sus objetivos. Cabe recalcar que el contexto es importante puesto que determina el tipo de poder que requiere el actor (Keohane & Nye, 1977). Dentro del ciberespacio, se debe tener en cuenta el flujo de la información y quién la posee para poder determinar el poder de un actor, así también evaluar los costos y beneficios que proporciona debido que las asimetrías se encuentran atenuadas en el ciberespacio (Nye, 2010) .

Este subcapítulo explora de manera exhaustiva el poder y su distribución, pues existen más actores que influyen en la toma de decisiones del sistema internacional, cambiando la concepción de poder y transfiriéndolo a varios actores. De igual manera, se analiza la importancia de las nuevas tecnologías en el uso y recursos de poder, visto que, en especial, el internet modifica los comportamientos de los actores y los incita a desenvolverse en diferentes ámbitos.

1.5.1. El rol de Estado eclipsado por las instituciones

En la interdependencia, el poder cambia su estructura lo que altera la distribución del mismo. Nye (2003) establece los términos de la transición y difusión del poder. La primera se refiere al hecho que el poder puede residir en los Estados más débiles, o que poseen menores capacidades militares. Por otro lado, la difusión del poder describe el traspaso de poder de Estados a actores no estatales. Se puede observar, entonces, tres fenómenos suscitados gracias a la globalización: el rol del Estado, nuevos actores, la agenda global que se deriva de la lucha de poder de los actores.

El rol del Estado

El modelo estatocéntrico o que basa sus principios en las relaciones meramente interestatales perdió sentido después de la globalización. El modelo actual es multicéntrico, pues los Estados cada vez son ineficaces, por su cuenta, al momento resolver las problemáticas económicas, sociales y políticas que garantizan el bienestar de su población. El Realismo concibe al poder como una capacidad material, sin tomar en cuenta las relaciones sociales donde se encuentran la convergencia de individuos, intereses, estructuras, normas y valores que determinan al Estado en su comportamiento. El surgimiento de nuevos actores externos al Estado y las nuevas problemáticas alteran las relaciones y los Estados no pueden actuar por sí mismos (Acevedo, 2013).

La realidad de la desaparición de las fronteras no solo físicas sino entre lo interno y externo afecta al Estado y su soberanía. Los Estados dejan de ser completamente autónomos y no pueden decidir sobre sus territorios sin pensar antes en las repercusiones de sus decisiones sobre otros actores, sean Estados o no. Por lo tanto, estos están casi obligados a crear alianzas para la resolución de conflictos, lo cual los compromete a ceder parte de su poder tanto interno como externo para sobrevivir en el nuevo sistema internacional (Acevedo, 2013).

Actores no estatales: instituciones

El cambio en la estructura del poder permite que las instituciones influyan en la política mundial, adquiriendo importancia al canalizar la cooperación y atenuar los efectos que derivan de la anarquía del sistema internacional. Es así que estas moldean el uso de poder, sin invalidar las asimetrías existentes pero acentuando los puntos fuertes de los actores. La ventaja de las instituciones dentro del ejercicio del poder es el uso del *soft power*, que de esta manera influyen en la toma de decisiones a largo plazo (Creus, 2013).

La existencia de canales múltiples que permiten la vinculación de Estados débiles con Estados fuertes, así como de individuos y organismos no gubernamentales a la política mundial. El papel de los organismos internacionales, entonces se convierte en un eje necesario para la resolución de conflictos mundiales como mediadores. Estos influyen en la constitución de la agenda internacional como catalizadores de las coaliciones para dar paso a las iniciativas políticas los Estados que no poseen poder militar, aquellos que el Realismo considera débiles. De la misma manera la participación de los organismos al interior del gobierno favorece a establecer prioridades en las problemáticas gubernamentales poniendo énfasis en la igualdad social y económica (Keohane & Nye, 1977).

De esta manera, las instituciones moldean preferencias adentrándonos en la tercera dimensión, por lo tanto, el desarrollo de las instituciones a nivel mundial va en aumento. El sistema internacional se encuentra en una era donde las instituciones han tomado un papel altamente importante, pero que todavía fallan al resolver conflictos. Esto no es desfavorable, simplemente muestra la complejidad de los fenómenos suscitados con la globalización y la creciente dependencia en las instituciones, que a su vez trabajan para mejorar sus actividades creando más transparencia, publicando más información y creando organismos adjuntos que supervisen su desempeño. Sin embargo, las fallas se adjudican también a las asimetrías, pues ciertos Estados han logrado influenciar las decisiones tomadas por las instituciones, priorizando sus intereses (Stone, 2008).

Se puede citar el caso de Malasia que en 2011 logró crear la institución, IMPACT[4], especializada en la detección y eliminación de amenazas cibernéticas para un posterior perfeccionamiento de las políticas mundiales de ciberdefensa. Esta alianza es respaldada por Naciones Unidas y funciona en más de 150 países

[4] International Multilateral Partnership Against Cyber Threats: primera alianza de ciberseguridad avalada por Naciones Unidas.

que, a través de expertos desarrollan soluciones para estas nuevas amenazas (IMPACT, s.F).

La hegemonía en la interdependencia compleja

El poder es una herramienta que permite a los actores obtener los resultados deseados, es decir un recurso; por lo tanto, cuando existe una preponderancia de recursos, un Estado obtiene las capacidades para influir dentro del orden mundial y está dispuesto a gobernar las relaciones entre países: a esto se le conoce como hegemonía. Dentro de un mundo interdependiente, la hegemonía varía desde su perspectiva original, pues la creación de instituciones permite que los actores cooperen sin dejar de lado sus intereses. De esta manera, Keohane considera que la hegemonía produce reglas, instituciones y regímenes que se traducen en cooperación y estabilidad del sistema (Santana, 2017).

La hegemonía desde la perspectiva interdependiente se da cuando los actores del sistema aceptan que existen beneficios del orden hegemónico lo cual crea una legitimación donde hay una situación de estabilidad y mutuos beneficios. Para el autor, el declive de una hegemonía no significa que el orden imperante se esté desvaneciendo, sino que es una transformación del poder que el hegemón ejerce (Santana, 2017). Las instituciones y la cooperación son las encargadas de brindar la estabilidad que existía previamente, dentro de la cual existen actores principales y periféricos. Incluso se puede señalar que la hegemonía depende de una cooperación asimétrica, la cual los Estados hegemónicos exitosos logran mantener (Keohane, 1984).

Por lo tanto, se puede hablar de una hegemonía ideológica, la cual no es una imposición del poder del hegemón sino que se deriva del mismo principio de estabilidad y mutuos beneficios. Esta nueva forma hegemónica estaría conformada por soberanías superpuestas y redes de poder, que impiden una hegemonía absoluta o jerarquías determinantes. De esta manera, según la

propuesta de Keohane, la hegemonía se convierte en un intento de posicionar una política de poder de un Estado dentro del sistema internacional (Keohane, 1984).

1.5.2. El ciberespacio: el poder de difusión de la información

La globalización transformó el mundo tanto en la parte social, política y ecológica como económica y militar, pero lo que realmente revolucionó la escena mundial es el desarrollo tecnológico. El rápido avance de la tecnología permite que la información, de cualquier tipo, se transmita de manera instantánea y a tiempo real. El ciberespacio es sin duda el invento más importante y el cual ha llegado a espacios comunes[5] (Bejarano, 2013). En el contexto de la política mundial, el ciberespacio es primordial debido a su reducido precio de entrada, anonimato y las asimetrías que se acentúan. En la política cotidiana, los individuos son capaces de ejercer sus derechos de manera limitada, en el ciberespacio sus capacidades se intensifican y las características propias de este lo vuelven casi invencible si sabe cómo explotarlas al máximo (Nye, 2010).

El poder de difusión es un proceso complejo, visto que la era de la información provoca un fenómeno donde los actores, en especial los Estados no tienen control sobre lo que sucede a su alrededor. Según autores como Avin Toffler (1995) y Esther Dyson (1998), el rápido desarrollo de la información podría provocar que en un futuro distante las jerarquías burocráticas sean reemplazadas con organizaciones de redes[6], los temas económicos asumidos por empresas privadas e incluso el espacio social será formado de manera virtual destruyendo las fronteras territoriales y desarrollando nuevos patrones de gobernanza, convirtiendo en obsoleta la figura de Estado. A pesar de que sus visiones pueden ser demasiado ilusorias, hay que dar crédito a la revolución que provoca en las estructuras de poder la aparición del ciberespacio y las posibilidades que este presenta (Nye, 2010).

[5] Global Commons: espacios comunes conocidos como mar, tierra, aire y espacio (Bejarano, 2013).
[6] Organización de redes: una estructura donde las acciones son llevadas a cabo por un grupo de personas o instituciones sin jerarquía (Ronfeldt, 2001).

El Estado continúa siendo el actor dominante, incluso en el ciberespacio, lo que no impide que existan varios actores que ejercen influencia y control sobre el mismo. La información significa poder, por lo tanto los gobiernos tratan de reservar ciertos datos que podrían beneficiar a otros actores y disminuir su propio poder. El objetivo del ciberespacio entonces se convierte en uno amenazante para el Estado, puesto que la tecnología avanza a pasos apresurados, tanto que los gobiernos no pueden alcanzarla. La información se difunde a una velocidad sin precedentes que inutiliza las acciones de los Estados debido a que los costos de creación versus los de formulación de leyes y control son mucho menores y cada vez disminuyen más (Nye, 2010).

En el siglo veintiuno, los costos computacionales se redujeron a una milésima del costo que tenían en 1970; de la misma manera, a principios del año 1993 la cantidad de páginas web existentes no excedía las 50, pero a finales del mismo año incrementó al punto de sobrepasar las 5 millones de páginas. China en 2010 tenía cerca de 400 millones de usuarios y la información digital aumentaba diez veces su tamaño cada cinco años. Cabe recalcar que su almacenamiento también evolucionó por lo que en 1980 una giga de información cabía en un cuarto entero, actualmente 200 gigas caben en un pequeño dispositivo que puede ser fácilmente trasladado en un bolsillo (The Economist, 2010).

El poder basado en recursos de información no es un término nuevo, pero el ciberpoder sí. "Ciber" representa toda actividad relacionada con computadoras y aparatos electrónicos. Por lo tanto el poder del ciberespacio recae en los recursos y capacidades derivados del uso de este dominio. En efecto, en 1969 el Departamento de Defensa creó la conexión de unas pocas computadoras, ARPANET, en el año 1972 se empezó a intercambiar información a través de códigos informáticos; el primer dominio de internet se crea en 1983 y con ellos los primeros virus. En 1989 se creó la Red Mundial y Google, el motor de búsqueda más popular actualmente, se fundó en 1998. Para finales de los 90, las compañías empiezan a utilizar internet para desarrollar el mercado y las cadenas de suministro global (Nye, 2010).

Nye (2010) define al ciberpoder como “la capacidad de obtener los resultados deseados mediante el uso de los recursos de información interconectados electrónicamente en el dominio cibernético” (pág. 3). Kuehl (2014) amplía más la definición como “la capacidad de utilizar el ciberespacio para crear ventajas e influir en los acontecimientos en otros entornos operativos y a través de los instrumentos de poder.” (pág. 38) El ciberespacio entonces puede ser usado para obtener los resultados deseados dentro del mismo o usar sus herramientas para lograr los mismos objetivos en cualquier otro dominio (Nye, 2010).

El conflicto presente en el ciberespacio se manifiesta de manera más acentuada para los Estados, que crean dependencia de las herramientas tecnológicas, lo cual para ellos representan mayores vulnerabilidades que otros actores pueden explotar a su conveniencia. En el mundo virtual los actores son varios y muchos anónimos, no existe una distancia medible y los ataques virtuales casi no tienen un costo; cabe recalcar que esto se da porque internet fue diseñado para que fuera fácil utilizarlo y no para mantener la seguridad. Por lo tanto, un actor, considerado fuerte no tiene las habilidades necesarias para desarmar o destruir un enemigo o hacer uso de manera efectiva sus estrategias de defensa (Nye, 2010).

Ejercer poder en el ciberespacio requiere de siete puntos estratégicos: sistemas operativos, motores de búsqueda, infraestructura física de telecomunicación, servicios de almacenamiento, foros de gobernanza, criptografía propia de internet y su protocolo. En cuanto al primero, sistemas operativos, a pesar que el ciberespacio carece de una autoridad, existen empresas que ejercen influencia como Microsoft y Apple. En cuanto a los motores de búsqueda, es decir aquellos que deciden las información que será publicada al momento que un usuario busque datos de interés, por lo tanto Google conquista internet con el 83% del mercado. La infraestructura de comunicación o los proveedores de internet ejercen influencia siempre y cuando puedan de cierta manera monopolizar el

mercado y vender sus servicios a nivel mundial. Los servicios de almacenamiento demuestran la confianza del usuario en la compañía, pues muchas empresas recopilan información sensible en estos servidores. La gobernanza, criptografía y protocolo hacen referencia específicamente al uso del ciberespacio (Bejarano, 2013).

De la misma manera que en otros dominios, en el ciberespacio se usan tanto las estrategias de *hard power* como de *soft power*. Debido a la falta de límites territoriales en el ciberespacio, es común para los actores disputar por abarcar mayor zona de influencia. Una estrategia expansionista proporcionaría mejoras económicas y de seguridad. Sin embargo, dentro del ciberespacio es más común encontrar el uso del *soft power*, ya que parte de la esencia de este es el establecimiento de relaciones por lo que los actores tratan de usar estrategias de atracción y cooperación. Esto no quiere decir que no existan estrategias propias del *hard power*, dado que el ciberespacio tiene acceso a otros dominios, es muy común que actores que no han conseguido imponer sus intereses de manera diplomática, utilicen ataques para extraer información de sus oponentes (Bejarano, 2013).

Un claro ejemplo de esta situación es el espionaje ruso a los sistemas cibernéticos de varios países de la Unión Europea y América Latina, y también Estados Unidos. Mediante el uso de un programa denominado Planeta, que opera en una red mundial de servidores se sustrae información confidencial que proporcionaría una ventaja en las negociaciones, tanto económicas como asuntos políticos de Rusia con los países afectados (Semana, 2014).

La evidencia de *hard power* encontrada en el ciberespacio a través del uso de ciertos puntos estratégicos incluye la denegación del servicio, arresto, prevención de la difusión de ciertos artículos por parte de blogueros o ciberactivistas o amenazas a los mismos. Estas herramientas representan una amenaza a la seguridad, lo cual perjudica el desarrollo libre y el progreso. Dentro del ciberespacio las amenazas, a pesar de no ser tangibles, afecta la seguridad

militar, política y económica. Esto se da mediante el acceso a información confidencial de un Estado, poniendo en riesgos sus estrategias nacionales. Además, se puede acceder a los sistemas y redes de la industria militar, exponiendo sus tácticas defensivas y accediendo a elementos tecnológicos militares con capacidad de ataque (Fink, 2010).

Por otro lado, el *soft power* se encuentra presente en campañas para modificar las preferencias de hackers así como para la población en general. Dado que esta herramienta tiene la característica de alcanzar los lugares más remotos y almacenar información, aún si ha sido borrada, se la puede considerar una de las mejores armas que tiene un actor para ejercer el cumplimiento de sus intereses y demandas (Nye, 2010).

1.2.3. Los recursos de poder en el ciberespacio

Existe una diferencia esencial entre el ciberespacio y sistema internacional, en relación al poder cualquier actor puede llegar a ejercer influencia en el ciberespacio, desde un individuo que tengan amplios conocimientos en informática hasta un Estado grande. En efecto, los actores pequeños son aquellos que más ventajas tienen gracias al fácil acceso y anonimato presentes. Cabe recalcar que son los individuos y asociaciones terroristas aquellos que causan más daño, por ejemplo el virus lanzado por un hacker Filipino causó 15 mil millones en daños, o en 2008 el cibercrimen se atribuyó un trillón de dólares en la sustracción de información y propiedad intelectual. De esta manera internet sirve a grupos terroristas para reclutar nuevos miembros y los activistas los usan para irrumpir en las páginas web de compañías y gobiernos. Por lo tanto, el ciberespacio estrecha la brecha entre el Estado y los actores no estatales, aun así se debe tener en cuenta que los Estados todavía poseen varios recursos (Nye, 2010).

Se puede dividir a los actores en tres categoría principales: gobiernos, organizaciones con redes estructuradas, e individuos con redes poco estructuradas (Nye, 2010).

Gobiernos

El gobierno posee varios recursos tanto económicos, políticos y físicos. Como se estableció previamente, existen siete puntos estratégicos que influyen en la determinación del poder de un actor; es así que la infraestructura física se mantiene delimitada por los límites territoriales, por lo tanto los gobiernos tienen jurisdicción. Estos pueden controlar los subsidios al desarrollo de infraestructura, educación informática en colegios públicos y la protección de la propiedad intelectual lo que puede determinar las capacidades de otros actores. Por otro lado, los gobiernos también son responsables de proveer un ambiente propicio para el desarrollo comercial a través de la aplicación de leyes que protejan y regulen las actividades dentro del ciberespacio de las organizaciones. Si el gobierno logra conseguir mediante estas herramientas una reputación legítima y competente, podrá mejorar su *soft power* dentro del ciberespacio (Nye, 2010).

Por otra parte, los gobiernos también pueden ejercer *hard power* a través de la coerción y control legal, visto que al detectar anomalías se puede privar del servicio de internet y comunicaciones zonas enteras. Aquellos gobiernos que tienen jurisdicción sobre grandes mercados pueden ejercer poder extraterritorialmente. Los gobiernos que detectan irrupciones en sus sistemas o actividades terroristas pueden llevar a cabo ciberataques o espionaje desde escaneos de puestos hasta alterar sitios web que han sido diseñados para causar destrucción física (Nye, 2010).

Organizaciones (sistemas altamente desarrollados)

Los ataques cibernéticos que suspenden el servicio o lo interrumpen pueden ser acciones realizadas por actores no estatales, pero dichos ataques se consideran de bajo costo cuando el objetivo son sitios web, pero un ataque al sistema de defensa de un gobierno requiere de una alta inversión en equipos y sistemas para descifrar la encriptación. Debido a esto se debe diferenciar el poder de difusión versus el poder de ecualización; el primero se refiere al control sobre la información publicada en el ciberespacio, mientras que el segundo se refiere a

que las capacidades que le da el ciberespacio a los actores los pondrían en las mismas condiciones (Nye, 2010).

Algunas empresas multinacionales y transnacionales pueden tener mayores recursos económicos y humanos que los gobiernos, y les permite explotar los mercados y los recursos en todo el mundo. Sin embargo, los gobiernos incentivan a este tipo de empresas a conservar su estatus legal y valor de la marca para que sigan cumpliendo con la estructura legal local. Por lo tanto, las empresas siguen respondiendo a los gobiernos (Nye, 2010).

Individuos y organizaciones criminales

Las estructuras legales no llegan a limitar a las organizaciones criminales. Muchas de estas basan sus operaciones en la estrategia de "*strike and exit*", lo que les permite obtener rápidas ganancias sin ser detectados a tiempo. Otras organizaciones tienen un carácter transnacional ya que se presume están financiadas o protegidas por gobiernos pequeños para extraer información y aumentar sus capacidades. Para las organizaciones terroristas es mejor operar en el ciberespacio que de manera física, con el objetivo de ocasionar un daño directo sin comprometer su identidad. Sin embargo, atacar los sistemas financieros y eléctricos de un país precisa de habilidades y equipos altamente sofisticados, por lo tanto los terroristas se concentran en objetivos más pequeños o usan el internet para promover el terrorismo (Nye, 2010).

TABLA 1
RECAPITULACIÓN: ACTOR Y SU RECURSO DE PODER EN EL CIBERESPACIO

Gobiernos	**Organizaciones**	**Individuos**
- Desarrollo e inversión en infraestructura, educación y propiedad intelectual - Coerción física y legal - Control de acceso y mercado	- Presupuesto y recurso humano - Flexibilidad transnacional - Control de código y desarrollo de productos - Marca y reputación	- Bajo costo de inversión - Fácil acceso - Anonimato y facilidad de salida - Vulnerabilidad asimétrica

- Capacidad de ciberataque y defensa - Proveer servicios públicos de regulación - Ejercicio de *soft power*		
Vulnerabilidad		
- Alta dependencia - Estabilidad política - Reputación	- Leyes regulatorias - Robo de propiedad intelectual - Irrupción de los sistemas -Reputación	- Coerción legal de ser atrapados

Fuente: (Nye, 2010) Elaboración: Camila Fuentes

1.3. *Smart power*: aplicación de la inteligencia contextual

En 2003, Joseph Nye desarrolla el término de *smart power* al llegar a la conclusión que la utilización de los dos poderes por separado no producen los resultados deseados, y que la combinación estratégica de ambos pueden llegar a crear escenarios óptimos. Sin embargo, para desarrollar un *smart power* eficiente se necesita de una inteligencia contextual, es decir tener conocimiento del contexto tanto interno como externo para poder formular políticas (Nye, 2009).

Las críticas a esta teoría son muchas, desde su origen suponen un ideal egoísta basado en recuperar la supremacía estadounidense. A pesar de que en teoría, sus postulados son coherentes y favorables, este no profundiza o supera las limitaciones del *hard* o *soft power*. Por lo tanto, en la misma teoría no se conocen los resultados de tomar decisiones basados en el *soft* o *hard power*, ni se toma en cuenta la conducta o preferencias de los actores. Dado que es un concepto que se ha desarrollado recientemente, no tiene una discusión profunda que aporte al uso del mismo, cabe resaltar que su aplicación resulta compleja por la falta de detalles y su ambigüedad (Coto, 2012).

Esta sección introduce el término del *smart power*, el cual presenta un nuevo cambio en la política exterior, estrechamente relacionado con la teoría de la Interdependencia Compleja, dado que sus bases surgen de la misma. La teoría

al ser contemporánea todavía requiere un análisis profundo que determine sus características principales y la forma de aplicación en la política. Finalmente, este apartado expone las críticas realizadas al término.

1.3.1. Aplicación del *smart power* a la política exterior

La Guerra contra el Terrorismo[7] fue la estrategia nacional desarrollada por George W. Bush después del ataque terrorista del 09 de septiembre del 2001 a las Torres Gemelas, centro financiero de Estados Unidos. A pesar de ser una medida tomada para derrotar a la organización terrorista Al-Qaeda y otras organizaciones, la estrategia de Bush afectó gravemente la imagen de los Estados Unidos frente al mundo (Lugo, 2003). El uso excesivo de la fuerza militar en la política exterior en los ataques dirigidos contra Afganistán e Irak provocó un descontento con el liderazgo norteamericano, tanto de sus ciudadanos como en el sistema internacional (Nye & Armitage, 2007).

Estados Unidos siempre ha sido reconocido como un líder mundial, sin embargo sus estrategias ofensivas ponían en tela de duda la legitimidad de este título. Joseph Nye, en 2003 desarrolla el término *Smart Power* como estrategia para reestablecer la hegemonía estadounidense. En la época de los 90, el mismo autor definió al *soft power* y estableció la importancia de su uso en la política doméstica y exterior, sin embargo entendió que su uso exclusivo no era suficiente para la resolución de conflictos. Existen tres maneras de obtener poder: la coerción, pago y persuasión. El *hard power* hace uso de las dos primeras, mientras que el *soft power* de la última. Por separado, los poderes llegan a establecer cierta influencia, pero para obtener los resultados deseados es necesaria la combinación de ambos (Nye & Armitage, 2007).

El *soft power*, en la era de la información aporta al diálogo político mundial para encontrar soluciones a los nuevos desafíos a través de la cooperación. Sin embargo, existen diferentes conflictos como en Medio Oriente donde el recurso

[7] Global War on Terror: la Estrategia Nacional para Combatir el Terrorismo se concentra en identificar y desactivar las amenazas antes de que lleguen a nuestras fronteras (Lugo, 2003)

del *soft power* no es suficiente y se deben aplicar sanciones económicas y hacer uso de la fuerza. Es de esta manera que la falta de balance entre los dos poderes insta a los actores a combinar de manera integral ambos. La esencia del *smart power* consiste en la capacidad de considerar y coordinar los intereses multilaterales de la cooperación internacional (Havrylenko, 2015).

Por otro lado, el *hard power* se refiere al uso de las habilidades económicas y militares que posea un país para ejercer influencia en otro actor. Éste usa la coerción, amenazas tanto en la parte económica como militar, así también un actor puede ofrecer protección militar o la reducción de barreras comerciales a cambio de lograr sus objetivos. De la misma manera que el *soft power*, este no se puede aplicar a todos los casos ya que puede mostrarse como una solución demasiado rígida que no llegue a obtener resultados favorables (Nye, 2009).

TABLA 2
RECAPITULACIÓN: *SOFT POWER* Y *HARD POWER* EN LA ESTRATEGIA DEL *SMART POWER*

Soft power	*Hard power*
• La cultura: cuando es agradable a otros • Sus valores: cuando son atractivos y consistentemente practicados • Sus políticas: cuando son inclusivas y legítimas	• Recursos militares: coerción y uso de la fuerza, amenazas • Recursos económicos: sanciones, amenazas.

Fuente: (Nye, 2009). Elaboración: Camila Fuentes

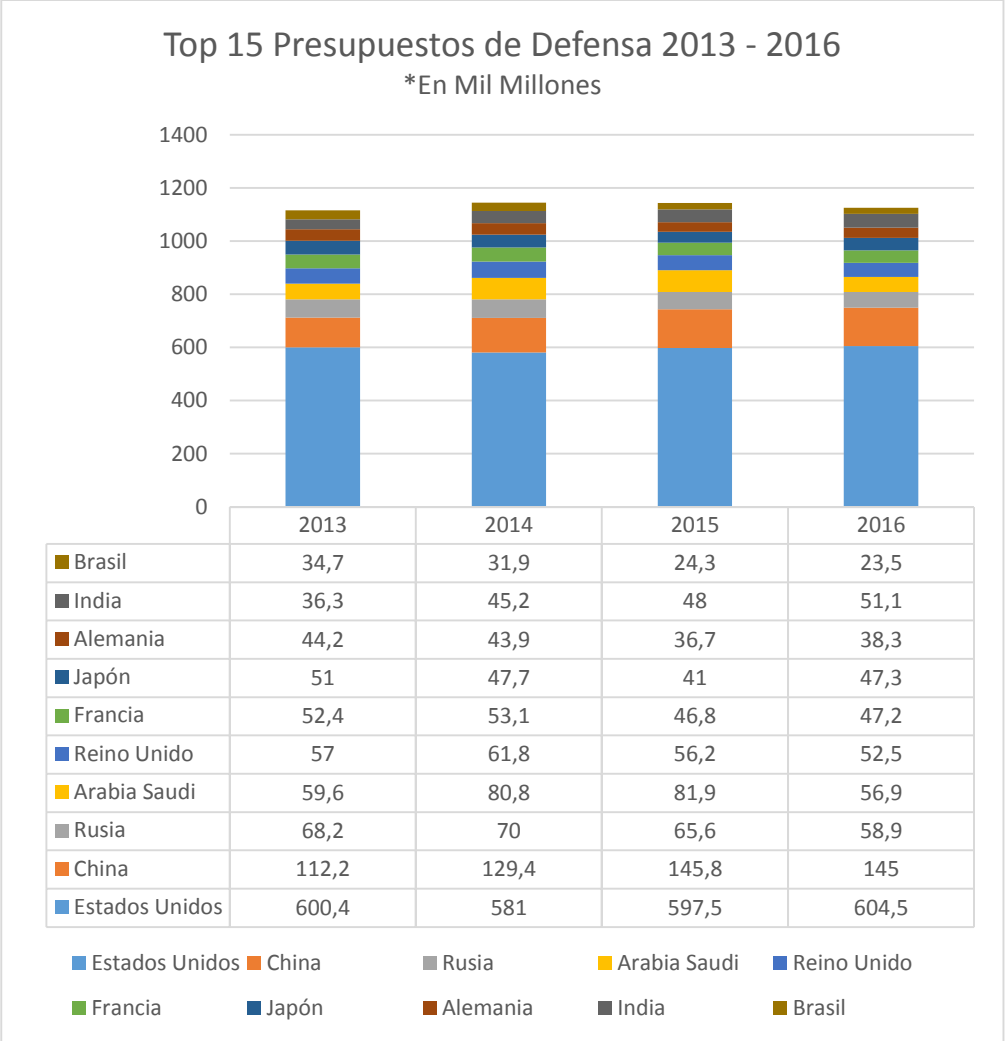
En 2007, el secretario de Estado, Richard Armitage y Joseph Nye conforman una comisión en el Centro de Estudios Internacionales y Estratégicos para popularizar el concepto y demostrar sus beneficios en la política exterior. Dentro de su explicación, Nye establece que para obtener un balance entre ambos poderes, se necesita tener inteligencia contextual. Para un mejor entendimiento de la misma, Nye comparó los niveles donde actúa la política internacional con un juego de ajedrez de tres dimensiones (Nye, 2009).

Inteligencia contextual: juego de ajedrez de tres dimensiones

El *smart power* se desarrolla de manera eficiente si se pone en práctica la inteligencia contextual, la cual explica que se debe hacer el uso de las habilidades diagnósticas intuitivas que permiten formular las políticas en base a los objetivos planteados por esta estrategia. A fin de obtener los resultados deseados se debe realizar un análisis de las fortalezas y debilidades, sin embargo es necesario conocer los tres niveles donde actúa el poder en la política internacional. Estos actúan explicando la unipolaridad o multipolaridad de las relaciones que determina el actor que posee el poder, dependiendo de su posicionamiento en las distintas dimensiones. El primero donde actúa el nivel militar, el segundo en las relaciones económicas y finalmente, el último nivel de las relaciones transnacionales (Nye, 2009).

El primer nivel donde actúa el poder hace referencia al *hard power*, el uso de la fuerza militar. Dentro de este nivel se maneja aún la unipolaridad, donde el poder lo posee Estados Unidos, en el Gráfico 1 se puede observar que invierte un promedio de 600 mil millones de dólares al año en el desarrollo de su industria militar, tanto en tecnología como capacitación, reclutamiento e investigación. Se puede observar que otros países invierten en gran medida en la industria militar, pero no a la dimensión de Estados Unidos que representa aproximadamente el 50% de la inversión mundial (Nye, 2009).

GRÁFICO 1
COMPARACIÓN PRESUPUESTOS DE DEFENSA ENTRE 2013 - 2016

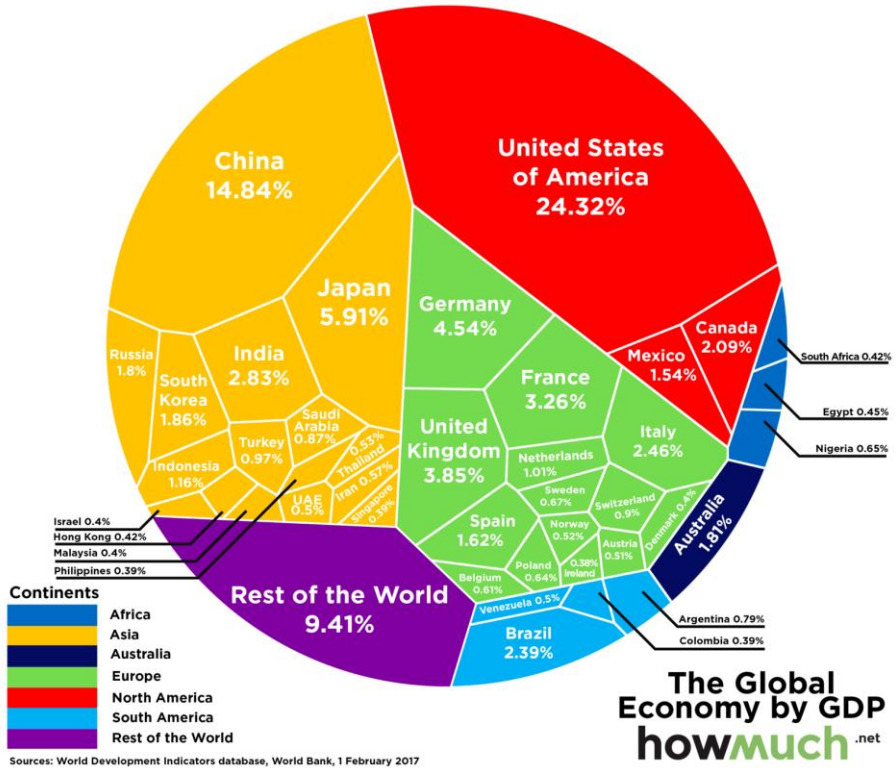


	2013	2014	2015	2016
Brasil	34,7	31,9	24,3	23,5
India	36,3	45,2	48	51,1
Alemania	44,2	43,9	36,7	38,3
Japón	51	47,7	41	47,3
Francia	52,4	53,1	46,8	47,2
Reino Unido	57	61,8	56,2	52,5
Arabia Saudi	59,6	80,8	81,9	56,9
Rusia	68,2	70	65,6	58,9
China	112,2	129,4	145,8	145
Estados Unidos	600,4	581	597,5	604,5

Fuente: (IISS, 2016). Elaboración: Camila Fuentes

El segundo nivel abarca las relaciones económicas interestatales, dentro de este nivel existe la posibilidad de un multilateralismo dado que existen economías que han crecido en los últimos años de manera constante y comienzan a competir entre sí (Nye, 2009). En el Gráfico 2 se observa que Estados Unidos continúa ostentando el poder económico mundial, mientras que sus rivales son China, Japón y Alemania, sin embargo se encuentran lejos de obtener el poder del primero, que representa el 24,32% de la economía, es decir la cuarta parte, mientras que China le sigue con el 14,84% (World Economic Forum, 2017).

GRÁFICO 2
COMPARACIÓN PORCENTAJES DE LAS ECONOMÍAS MUNDIALES



Fuente y Elaboración: (World Economic Forum, 2017)

Finalmente, el tercer nivel hace referencia a las relaciones transnacionales que comprende temas ecológicos, terrorismo, narcotráfico, activismo, etc. Dentro de este nivel no integran solamente Estados, sino también actores no estatales, por lo que el poder se dispersa y depende del contexto para poder analizarlo de mejor manera. Frente a los nuevos desafíos presentes en el mundo se requiere el uso de estrategias apropiadas para cada uno (Nye, 2009).

1.3.2. Características del *smart power*: armando la estrategia

Joseph Nye y Richard Armitage (2007) dentro de la publicación "*A smarter, more secure America"* definen una estrategia para los futuros presidentes de Estados Unidos. La publicación comprende un análisis de la situación de Estados Unidos en el momento y una serie de recomendaciones que incluyen la cooperación internacional, desarrollo global, diplomacia, integración económica y tecnología e innovación. El objetivo principal es restaurar la confianza interna y externa en el gobierno de este país.

Las políticas estadounidenses han sido muy criticadas tanto por los ciudadanos como por aliados y adversarios del país debido a la severidad presente en las medidas tomadas para combatir el terrorismo. En 2007, *World Public Opinion Poll* demostró que 10 de los 15 países encuestados han perdido la confianza en Estados Unidos; de la misma manera la BBC en el mismo año realizó una encuesta que reveló más de 26,000 personas de los 25 países encuestados tienen una imagen negativa de este país. Por lo tanto, el gobierno estadounidense se ve en la búsqueda de estrategias para contrarrestar estos efectos, pues la influencia y confianza en el país permite una estabilidad tanto en temas económicos como de seguridad (Nye y Armitage, 2007).

Los autores determinaron que existen cinco causas principales del declive de la influencia estadounidense; en primer lugar el status de superpotencia que adquirió después de la Guerra Fría. Esto convirtió a Estados Unidos en un objetivo ya que otros países consideraron que el sistema internacional no debería ser unipolar y que su poder era ilegítimo. En segunda instancia, Estados Unidos es visto como el promotor de la globalización y el desarrollo de la tecnología, lo cual provocó que muchos países tengan que realizar ajustes en sus políticas internas y externas para adaptarse a las nuevas reglas impuestas. Además, el país comenzó a rechazar acuerdos internacionales para el progreso mundial sin proponer soluciones alternas a las nuevas amenazas (Nye y Armitage, 2007).

El cuarto tema, se convirtió en el punto de inflexión visto que Estados Unidos mantenía un poder legitimado por unos pero no por todos y al aplicar las medidas en respuesta al 9/11 dejó ver a un líder inseguro y asustado que prohibió la entrada a su país y de cierta manera mostro cierto discrimen hacia los extranjeros, lo cual incluso lo llevó a realizar acciones secretas que habían sido abiertamente desacreditadas cuando fueron realizadas por otros Estados. Finalmente, el proceso llevado a cabo desde finales de la Guerra Fría ha puesto en duda la eficacia de Estados Unidos como líder mundial. Previo a este suceso, el país estaba a la vanguardia de la tecnología y parecía que ningún conflicto era muy grande, pero los últimos años demostraron su incapacidad de hacerle frente

a los problemas. A pesar de todo el contexto previo, la idea que vende el país sigue siendo popular entre muchos, por lo que según los autores se debe aprovechar para comenzar una nueva estrategia dirigida a corregir las fallas establecidas previamente (Nye y Armitage, 2007).

Alianzas, sociedades e instituciones

Las amenazas actuales requieren de una estrategia que analice el problema a fondo, por lo tanto Estados Unidos tiene maneras diferentes de abordar los problemas. La primera es actuar de manera unilateral, lo cual le da libertad de acción pero afecta a su imagen en el sistema internacional, lo que puede llevarlo al aislamiento. De la misma manera, al actuar solo el financiamiento y beneficios operativos disminuyen. La segunda manera es hacer coaliciones donde exista un consenso por parte de los otros actores, lo cual permite a Estados Unidos estar exento de las restricciones impuestas por una alianza. El principal desafío que presenta es encontrar países que posean las mismas ideologías y trabajen en conjunto, así mismo las coaliciones de este tipo no permiten establecer estrategias para amenazas futuras por lo que se debe considerar como una solución a corto plazo. Finalmente, la creación de alianzas y organismos multilaterales que tengan normas y objetivos comunes, de esta manera se crea confianza y trabajo en equipo lo que llevó a Estados Unidos a tener una posición dominante frente a la Unión Soviética (Nye y Armitage, 2007).

La creación de alianzas puede traer beneficios a corto y largo plazo, en el primer caso ayuda a abordar situaciones sin tener que crear consensos con otros países, lo cual resulta favorable debido a la cantidad de amenazas actuales. A largo plazo, la inversión en instituciones y organismos internacionales ayuda a la preservación de los valores, ideas e intereses del país, y ayuda a forjar vínculos con otros actores. Naciones Unidas es el organismo más importante y por lo tanto requiere de mejoras constantes para establecer normas y objetivos duraderos que contrarresten el terrorismo y mantengan la paz en el sistema (Nye y Armitage, 2007).

La aplicación del soft power, mediante las alianzas e instituciones presenta una herramienta útil para la intervención no directa a los conflictos latentes. Sin embargo, una estrategia de *smart power* exitosa es aquella que logra diferenciar entre las audiencias. Saber diferenciar el momento de aplicar los diferentes poderes es crucial, por ejemplo la aplicación de la cooperación mediante instituciones y alianzas es posible en países que necesiten de asistencia; mientras que países que se encuentren en situaciones de extremo conflicto deberían ser abordadas desde otra perspectiva (Sonenshine, 2015).

Desarrollo global y diplomacia

Los esfuerzos de Estados Unidos por crear un desarrollo global han estado caracterizados por la inconsistencia, reflejado en la falta de políticas coherentes y una base fuerte y estable. El compromiso del gobierno con la asistencia para el desarrollo se ha visto eclipsado por la ayuda que presta la empresa privada y otros Estados. Se debe resaltar que lo que busca la estrategia del *smart power* es mejorar la calidad de la ayuda, más no su volumen. Por lo tanto, al observar los sucesos de las últimas décadas debido al terrorismo, es importante trabajar en conjunto tanto con otros Estados como con instituciones, organizaciones internacionales y la sociedad civil para la inversión en defensa y recuperación de los pueblos que han sido especialmente afectados por esta amenaza, lo cual requiere poner atención a diferentes frentes como la salud, economía y educación (Nye & Armitage, 2007).

Integración económica

El comercio es parte importante del desarrollo de Estados Unidos y lo ha posicionado como la economía más grande del mundo, que según el Banco Mundial (2016) alcanza un PIB anual aproximado de 17 mil millones de dólares. Sin embargo, la competencia económica ha ayudado a otras naciones a desarrollar sus capacidades y diversificar los mercados para reemplazar a Estados Unidos. La tecnología ha cambiado las bases de la economía, debido que se facilitan las

comunicaciones lo que ha transformado la cadena de suministro en un servicio esencial para el comercio. Así de esta manera, se busca invertir en educar a la nueva generación y que sea esta la que aporte con nuevas ideas al desarrollo. Se debe tomar en cuenta también que la diversidad cultural gracias a la migración ha permitido a Estados Unidos destacarse y estar a la vanguardia (Nye y Armitage, 2007).

Se requiere de una política de migración inteligente que se beneficie de las habilidades de los extranjeros que ingresen a este país. Debido a esto, es importante crear acuerdos internacionales y bajar las barreras de ingreso, siempre analizando las ventajas y deshacer. Por lo tanto, según los autores es importante que Estados Unidos tome el liderazgo de crear redes de comercio que sirvan al desarrollo global de la economía (Nye y Armitage, 2007).

La dependencia hacia la tecnología se ha convertido en parte crítica de la respuesta a las crisis, puesto que se puede intervenir a través de la misma. Por ejemplo, durante un terremoto mediante asistencia militar y las telecomunicaciones se puede iniciar la búsqueda de sobrevivientes; así mismo, los programas de televisión, videojuegos, entre otras cosas para educar a la población acerca de las acciones que se pueden tomar en casos de desastre (Sonenshine, 2015).

Tecnología e innovación

Estados Unidos ha estado en la vanguardia del desarrollo tecnológico, pero debido a los problemas medio ambientales que este provoca, es necesario crear una estrategia que comprenda el desarrollo, seguridad y sostenibilidad. Esto comprende el perfeccionamiento de la infraestructura, el marco legal que respete la soberanía de otros países y necesidades de los usuarios, y la cooperación (Nye & Armitage, 2007).

En 2014, el departamento de Energía de Estados Unidos dio a conocer el plan estratégico 2014 – 2018, que enumera los objetivos a cumplirse durante estos años. Las metas planteadas buscan un desarrollo sostenible de la tecnología, por ejemplo, la reducción de amenazas nucleares mientras que se generan nuevas fuentes de energía limpia que generen a su vez trabajo, seguridad y desarrollo económico (Department of Energy, 2018).

1.3.3. Críticas de la teoría: ¿realmente funciona?

El *smart power* es una estrategia nueva implementada para recuperar el poder de influencia de Estados Unidos en el mundo, algunos países adoptaron también la estrategia, sin embargo esta ha sido muy criticada. La estrategia toma en cuenta los dos poderes para actuar en la política exterior, por lo cual tiene un enfoque más completo, entiende que los dos por separado no logran obtener los resultados deseados. Por otro lado, las críticas se direccionan a la falta de una aplicación clara y fallas metodológicas (Coto, 2012).

Esta estrategia toma en cuenta elementos del poder militar, así como económicos, ideológicos y culturales lo que le permite analizar los objetivos y encontrar posibilidades para desarrollar una estrategia global a corto, mediano y largo plazo. El análisis desde ambas perspectivas permite pronosticar las tendencias y trabajar conforme a éstas utilizando la tecnología, que permite el flujo de información (Coto, 2012).

En segunda instancia, la estrategia permite profundizar el análisis de la realidad internacional que ayudan a desarrollar elementos analíticos como la inteligencia contextual. Para aplicarla de mejor manera se debe tomar en cuenta el contexto cultural, la distribución de recursos de poder, las necesidades y demandas de la ciudadanía, el tiempo y la información. Uno de los elementos más importantes es la información, gracias a la tecnología su acceso se da de manera fácil y sin barreras. A pesar de ser útil para los gobiernos al momento de la toma de decisiones, también permite que cualquier actor acceda al ciberespacio. Esto

ha provocado la filtración de información y ciberataques, así como el reclutamiento de terroristas y grupos adversarios a los gobiernos.

Por ejemplo, la inteligencia contextual entiende que un conflicto puede ser resuelto mediante mecanismos de paz, es necesario entender que el contexto del país en el que se interviene o con el cual existe el conflicto, ayudará a la resolución del mismo. Se puede evocar a la mediación, la cual lleva, en situaciones óptimas, a crear una paz positiva. Por lo tanto, la cultura, las necesidades y demandas de una población, la política, entre otras cosas son principios fundamentales que se deben tomar en cuenta para la creación de una estrategia (Sauceda, 2015). Sin embargo, existen casos en los cuales es imperativo determinar una acción fuerte o determinante, parte del poder duro, para terminar con una amenaza inminente (Wong-Diaz, 2013).

Por otro lado, el término ha sido muy politizado y tienen intereses dominantes ya que responde a las necesidades de Estados Unidos de retomar su puesto como líder mundial. Por lo tanto, toma como punto de partida la situación de Estados Unidos y no presenta estudios profundos que demuestren una base teórica valedera. Esta no profundiza en las limitaciones de ambos poderes y tampoco realiza una propuesta que mejore su aplicación. Incluso Nye estableció que la aplicación del *smart power* estaba limitado por las preferencias de los beneficiados u otros actores que podrían cambiar los resultados ya analizados. Además se hacen observaciones en cuanto a las asimetrías, pues no todos los países son capaces de aplicar la estrategia debido a que carecen de los recursos y capacidades. En conclusión, su aplicación es fácil en teoría pero al momento de ponerla en acción no obtiene los resultados previstos, si no se dispone de las capacidades necesarias (Coto, 2012).

En conclusión, el primer capítulo de esta investigación cumple el objetivo específico planteado, el cual busca analizar el concepto del *smart power* dentro de un sistema internacional anárquico donde el protagonismo de los Estados se ve afectado por individuos y actores externos. Bajo el marco de la interdependencia compleja, que reconoce un sistema anárquico y la existencia de nuevos actores no

estatales, se analiza la evolución de la política mundial y el cambio de su estructura. Esta teoría incluye temas sociales, ecológicos y económicos que modifican la toma de decisiones, dejando en un segundo plano a la seguridad y fuerza militar, por lo tanto revela la razón de una menor influencia por parte de los Estados en el sistema internacional, cabe recalcar que la teoría sigue siendo estatocentrista y analiza el rol de los Estados en este nuevo orden mundial. Además, se estudia la evolución de la naturaleza del poder, que no es único y su distribución es desigual debido a las asimetrías de los actores. La teoría toma en cuenta el grado de dependencia como causa de las ganancias o pérdidas, por lo tanto no se puede hablar de poderes absolutos sino relativos. La globalización se presenta como un punto de primordial para estos cambios, dado que incrementa el poder de la información y la comunicación, entonces surgen dos tipos de poder: *soft power* y *hard power*.

La globalización también dio paso al avance tecnológico, debido a su capacidad de difusión de información. El ciberespacio, uno de los inventos con mayor importancia para el sistema actual, disminuye más las asimetrías de los actores e incluso permite que actores no estatales se conviertan en amenazas al poder de los Estados, más no su hegemonía. Por lo tanto, estos se han visto en la necesidad de crear una estrategia que aborde las nuevas amenazas, mediante la combinación de ambos poderes. De esta manera el *smart power* es una estrategia de comienzos del presente siglo con el objetivo de reestablecer el poder estadounidense. Sin embargo, existen críticas direccionadas a la falta de una aplicación clara y una falla metodológica, así como los objetivos de la misma. Esto se da porque se trata de una estrategia que continúa en un proceso de evolución y es creada basada en la realidad estadounidense.

CAPÍTULO II

FILTRACIONES DE LA NSA: REPERCUSIONES EN LA POLÍTICA EXTERIOR CIBERNÉTICA ESTADOUNIDENSE

2.1. Antecedentes: filtraciones de WikiLeaks y medidas de defensa

Las amenazas del nuevo siglo se presentan igual o más complejas que las enfrentadas en el pasado, el terrorismo en todas sus formas se ha convertido en el desafío más peligroso. El 11 de septiembre del 2001, se perpetra el acto terrorista que marca la historia de Estados Unidos y el mundo. George Bush, presidente durante el siniestro, declara la "Guerra contra el Terrorismo"[8] con el claro objetivo de identificar y destruir a los responsables para proteger los intereses estadounidenses y globales (González, 2011). Casi una década después, el terrorismo había evolucionado, utilizando herramientas tecnológicas que permitían causar daños irreparables en distintas áreas (Obama, 2009).

Barack Obama (2009), señala en sus primeros discursos como presidente electo de los Estados Unidos que se fortalecerá la seguridad en el ciberespacio, reconociendo de esta manera que este medio se ha convertido en un arma tanto para los Estados como para grupos terroristas, pues la misma tecnología que los países usan para su progreso y defensa, la usan aquellos que quieren dañarlos (U.S. Army Cyber Command, s.F).

En este apartado presenta un preámbulo, pues describe un caso anterior similar al de Snowden. Expone los cambios que el presidente Barack Obama realiza con el cambio de gobierno, con políticas orientadas al respeto de los derechos civiles, inversión en educación y salud, y un enfoque especial en las nuevas tecnologías, principalmente dentro del ciberespacio. En contraposición, presenta a breves rasgos el caso de WikiLeaks, organización que logra infiltrarse en la información clasificada del gobierno de Bush y expone las actividades de

[8] *Global War on Terror*: la Estrategia Nacional para Combatir el Terrorismo se concentra en identificar y desactivar las amenazas antes de que lleguen a nuestras fronteras (Lugo, 2003)

espionaje y ataques en Medio Oriente. Finalmente, se hace referencia a las medidas que se tomaron para prevenir un suceso parecido.

2.1.1. Gobierno de Obama: el fortalecimiento de la ciberdefensa

El gobierno del presidente George W. Bush fue una era de cambios en temas de seguridad. El terrorismo se encontraba en su clímax y nuevas formas del mismo empezaban a incidir dentro del escenario mundial. Los virus de computadora y los ataques de denegación de servicios dejaron de ser un inconveniente pasajero que podía ser resuelto a cabo de horas y tan sólo presentaba molestias sin importancia. Estos instrumentos del ciberespacio se convirtieron en importantes armas que amenazan a la seguridad mundial, pues logran inhabilitar redes de Estados y denegar servicios, ahora considerados como básicos, para robar información e instalar sistemas de espionaje digital. Cabe recalcar que el sistema internacional se encuentra en una guerra cibernética que pasa casi desapercibida, pero que puede llegar a tener resultados más caóticos que una guerra física (OTAN, s.F.).

A finales de su período presidencial, Bush se enfrentó a uno de los peores ataques ciberterroristas, pues en 2008 se detectó en los sistemas informáticos militares estadounidenses la presencia de una memoria USB conectada a una de las computadoras de una base militar en Medio Oriente. La memoria contenía un poderoso programa de espionaje que tenía como característica propagarse sin ser detectado a través de la red militar analizando documentos clasificados y no clasificados, que fueron transferidos a servidores manejados por grupos extranjeros (OTAN, s.F.).

Obama asume la responsabilidad de cambiar esta realidad y mejorar la infraestructura digital para evitar futuros incidentes. En las observaciones del 2009 acerca de la ciberinfraestructura, Obama asegura que esta es una crucial herramienta para el desarrollo de la economía, la industria militar y el gobierno, pues la dependencia en la misma es muy grande y constituye la base para el progreso. De la misma manera, el ciberespacio también representa un arma

poderosa contra los gobiernos. De acuerdo a una encuesta realizada en 2008, los últimos dos años han representado una pérdida de 8 mil millones de dólares debido al cibercrimen. La ventaja de estos criminales es que el ciberespacio permite el acceso global y los actos criminales son perpetrados en un máximo de 30 minutos, algunos sin ser detectados (Obama, 2009).

En 2009, se condujo una revisión de las políticas del ciberespacio para identificar las fallas y mejorar las estrategias de defensa. Se llegó a la conclusión que el desarrollo de la infraestructura estaba impulsado por interoperabilidad y eficiencia, pero no enfocado en la seguridad. De la misma manera, se evidenciaron ataques de actores no estatales que atentaban con irrumpir o destruir los sistemas estadounidenses. Por lo tanto, se identificó que mientras se promueve la innovación, eficiencia, prosperidad económica y comunicación, también se necesita poner un énfasis especial en la defensa y seguridad, sin limitar los derechos civiles y la privacidad. Cabe recalcar que esto se logrará mediante el liderazgo mundial de Estados Unidos, el cual promoverá y empoderará las instituciones y departamentos federales para que realicen un trabajo eficiente coordinado por la Casa Blanca (Department of Homeland Security, 2009).

La estrategia se basa entonces en crear un plan donde las responsabilidades sean distribuidas de manera eficiente, y las organizaciones, sean de alto o bajo rango, puedan contribuir a la ciberseguridad. El objetivo principal es que no sea una sola institución la encargada de procurar la seguridad, sino que se inicie un trabajo grupal coordinado por el gobierno central. Es de esta manera que se estableció el Comité de Política Interagencial de Infraestructura de Información y Comunicaciones como el organismo organizador de políticas para un infraestructura confiable y segura, tanto de manera nacional como internacional. Para alcanzar las metas propuestas se necesita de una revisión de las políticas actuales, para que estas aseguren y asignen responsabilidades y roles de cada organismo (Department of Homeland Security, 2009).

La creación de una Nación Digital es necesaria para el progreso de la seguridad. Se debe crear consciencia entre los ciudadanos y las autoridades de los peligros y amenazas a los que se encuentran expuestos en internet. El gobierno iniciará una campaña nacional de concientización y educación, para el desarrollo de ciudadanos capaces de defender su información, así como ingenieros y científicos que aporten a la defensa nacional. Paralelamente, el entrenamiento y la capacitación del personal, así como el incentivo a organizaciones e individuos a tomar decisiones inteligentes en cuanto al ciberespacio. Sin embargo, para lograr los objetivos planteados, el gobierno de Estados Unidos no puede actuar en solitario. Es importante buscar la cooperación del sector privado, pues existen objetivos comunes que pueden llegar a ser alcanzados mediante la acción en conjunto. De la misma manera, se entiende que se debe trabajar en conjunto con otros Estados ya que se trata de una amenaza mundial que puede ser detectada mediante la cooperación (Department of Homeland Security, 2009).

2.1.2. WikiLeaks, las filtraciones de información clasificada

Un año después de comenzado el período presidencial de Obama, WikiLeaks filtró información clasificada de las actividades de Estados Unidos en Medio Oriente, las cuales mostraban torturas, asesinatos y ataques no registrados oficialmente. Este hecho puso en evidencia la crueldad con la que operaban los soldados estadounidenses bajo las órdenes de la Casa Blanca (Lopez, 2012).

WikiLeaks es una organización periodística internacional sin fines de lucro, fundada en 2006 por Julian Assange. La organización está compuesta por periodistas, analistas y expertos en redes que estudian y publican información censurada por los gobiernos con el objetivo de revelar los actos de corrupción, guerras y espionaje. Tienen contacto con más de 100 medios de comunicación internacionales que publican sus contenidos, permitiendo de esta manera crear el impacto necesario para que sus hallazgos lleguen a todo el mundo. Los valores de la organización están basados en la libre expresión y el derecho de los ciudadanos globales de estar informados (WikiLeaks, s.F.).

Fieles a su misión, WikiLeaks en abril de 2010 realizó la filtración de información más famosa acerca de Estados Unidos y sus operaciones en Medio Oriente. “Asesinato Colateral” es un video de aproximadamente 17 minutos que revela los ataques y asesinato por parte de las tropas estadounidenses en Irak a un grupo de personas presuntamente armadas acompañadas de dos periodistas de la agencia internacional de noticias *Reuters*. Después se puede observar que un civil iraquí intenta ayudar a estas personas mientras sus hijos esperan en un auto, es entonces que se lanza otra bomba que termina matando al civil e hiriendo a los menores. Se escucha también que la manera de expresarse de los soldados es altamente despectiva hacia los objetivos (Lopez, 2012).

Debido a que el video fue editado para poder ser enviado a los medios de comunicación, WikiLeaks publicó el video original de 39 minutos. No obstante, las partes no editadas mostraban una realidad ligeramente diferente, debido a que en una escena se observa a uno de los hombres atacados con lo que parece ser una granada, justificando de cierta forma las acciones del primer bombardeo. Cuando Assange fue entrevistado, manifestó que el objetivo de editar esta parte era crear polémica y mayor impacto político pues, el fundador de la organización critica el hecho que los gobiernos venden una idea falsa de la guerra y omiten en las cifras oficiales el verdadero número de muertes, que como se subraya en el video resultan ser colaterales. Así también señala el desprecio y falta de preocupación por la vida de menores y civiles inocentes (Lopez, 2012).

El soldado Bradley Manning, militar de inteligencia de alto rango, gracias a su nivel de acceso a las bases de datos de documentos clasificados fue el responsable de remitir a WikiLeaks el video e información clasificada. Por lo tanto, en julio del 2010 se hizo otra publicación de más de 90 000 documentos clasificados sobre los registros de la guerra en Afganistán en los cuales se evidencian las torturas, la violación a los derechos humanos, los asesinatos y las desapariciones de civiles. De igual manera, se muestran las misiones secretas para

terminar con la amenaza talibán y a Al-Qaeda, así como la cifra real de civiles muertos y ataques (Lopez, 2012).

En octubre del mismo año, se propagaron alrededor de 400 000 documentos de los registros de la Guerra de Irak que exponían las torturas hacia los detenidos iraquíes y cifras extra oficiales de víctimas civiles que sobrepasaban las 15 000. Se describía igualmente cómo las tropas estadounidenses tenían armas de última tecnología frente a los guerrilleros iraquíes que utilizaban armas improvisadas resultando en la destrucción casi total de ciudades como Faluya. Esta publicación fue el documento escrito y extendido del video "Asesino Colateral", que explicaba el contexto inmediato de la guerra, dando un visión completa de las acciones de la milicia estadounidense (Lopez, 2012).

Finalmente, se publicaron cables diplomáticos entre Estados Unidos y sus misiones y embajadas en el extranjero. En noviembre salió el primer set de 290 cables de 250 000, que fueron publicados gradualmente al cabo de seis meses. Las comunicaciones revelan las investigaciones y revelación de información de funcionarios de los países extranjeros, Naciones Unidas y planes de inteligencia. En las últimas revelaciones se mencionaba la detención ilegal de sospechosos en la prisión de Guantánamo, donde en 760 archivos revelan que inocentes fueron conducidos a las bases, sin presentar amenaza alguna, para ser interrogados mediante torturas sobre el terrorismo (Lopez, 2012).

2.1.3. Las repercusiones para Estados Unidos y su respuesta

Las filtraciones de WikiLeaks se enfocaron en gran medida en las actividades de Estados Unidos, lo cual tuvo un efecto en las operaciones militares, diplomáticas, la opinión pública y el poder e influencia del país en el mundo. Por lo tanto el gobierno de Obama realizó declaraciones y comenzó una campaña de desprestigio, principalmente en contra de Julian Assange (Lopez, 2012). El Almirante, Mike Mullen sentenció las acciones de Assange, señalando como irresponsable y emitió el siguiente comentario:

> *"El señor Assange puede decir lo que quiera sobre el gran bien que él y su fuente piensan que están haciendo, pero la verdad es que ya puede tener en sus manos la sangre de algún joven soldado o la de una familia afgana"(Levine, 2010).*

Declaraciones que fueron corroboradas cuando el portavoz talibán, Zabihullah Mujahid, anunció que se estaban analizando las publicaciones para identificar a miembros de sus tropas que hayan suministrado información a los estadounidenses. "Si son espías estadounidenses, entonces sabremos cómo castigarlos" (Winnett, 201).

Las filtraciones presuntamente ocasionarían efectos diplomáticos, debido que se nombraron a colaboradores que proporcionaban información clave, y de la misma manera se romperían relaciones por el espionaje. Uno de los casos más representativos sería el de México, cuando el embajador estadounidense, Carlos Pascual, manifestó su descontento y crítica hacia las acciones que tomaba el gobierno mexicano en cuanto al narcotráfico. Este hecho fue publicado en los cables diplomáticos, ocasionando en marzo del 2011, la renuncia del embajador estadounidense en México, el cual justificó su salida como una manera de mantener relaciones pacíficas con el país vecino (Lopez, 2012).

WikiLeaks generó una conciencia general acerca de la transparencia del gobierno, los ciudadanos empiezan a prestar atención y exigir que no se oculten las acciones sobre temas relevantes como el terrorismo y el crimen organizado. La polémica que surgió después de estas revelaciones provocó también malestar, pues se pone en debate los límites de la transparencia. En el caso WikiLeaks, sus críticos aseguran que se dieron más detalles de los necesarios, por ejemplo los nombres de las personas que actuaban secretamente para Estados Unidos, poniendo sus vidas en peligro; así como detalles de las tácticas de inteligencia que las agencias gubernamentales utilizaban y que su conocimiento general crea vulnerabilidad para el país (Lopez, 2012).

No obstante, WikiLeaks empezó a perder credibilidad por los escándalos suscitados durante y después de las filtraciones. Cabe recalcar que la organización

se puso en contacto con *The Guardian* y el *New York* Times, periódicos británicos y estadounidenses respectivamente, para la publicación de los documentos. Durante el análisis, Nick Davies, periodista investigativo de *The Guardian*, tuvo conocimiento que Assange había entregado los Diarios de Guerra de Afganistán y un resumen del contenido a ser publicado por el periódico (*The Guardian),* al canal de noticias Channel 4[9], Al Jazeera[10] y CNN[11], así como una entrevista pre-grabada para el primer canal. Esto significaba una violación directa a la exclusividad que habían pactado. Davies se retiró del proyecto mandando un claro mensaje a Assange, "No. No somos tus siervos. No estamos aquí para que las fuentes de información abusen de nosotros. Nosotros somos periodistas. No vamos a movernos siguiendo la cola del perro" (Lundberg, 2011).

David Leigh, director de investigaciones asumió el cargo de Davies, pero mostró su desconfianza y sigilo al continuar las operaciones. Por parte del *New York Times*, se decidió omitir la fuente de donde se obtuvo la información para mantener la credibilidad del diario, lo cual creó fricciones entre ellos y Assange. Para la segunda parte de las publicaciones, WikiLeaks atrasó las fechas de emisión para incluir a medios de comunicación televisivos, pero *The Guardian* aceptó bajo la condición de obtener los cables diplomáticos originales antes de la publicación para analizar si su contenido era de real interés (Lundberg, 2011).

Sin embargo, las últimas semanas de agosto del 2010 surgieron hechos que debilitaron la imagen de Assange, el cual se encontraba en medio de una demanda de dos jóvenes suecas acusándolo de acoso sexual. Este acontecimiento provocó la huida de Assange de Suecia hacia Londres, lo que cuestionaría aún más su credibilidad. Si bien sus publicaciones son de contenido relevante e informativo, muchos han criticado su estilo como poco novedoso, principalmente comparándolo con las filtraciones de los Pentagon Papers[12]. Además argumentan que WikiLeaks hace más énfasis en el espectáculo de las revelaciones que en la

[9] Televisión pública de Reino Unido
[10] Cadena de televisión de Catar
[11] Cable News Network canal de televisión privada estadounidense
[12] Compilación de documentos que revelan el intervencionismo estadounidense en Vietnam entre 1945 y 1967 que fueron revelados en el New York Times en 1971

verdad como tal, apoyándose en el show que Assange monta al dar declaraciones, entrevistas, ruedas de prensa, y en el mismo hecho de su victimización (Carrasco, 2010).

El segundo ciclo de publicaciones se realizó sin inconvenientes, pero Leigh durante una reunión social con su amiga periodista, Heather Brooke, se enteró que ella también había recibido los cables gracias al ex-programador de WikiLeaks, Smári McCarthy. Fueron noticias inquietantes para los directores del periódico, lo cual los llevó a tomar la decisión de compartir los cables con el *New York Times* y *Der Spiegel.* El trato entre Leigh y Assange se había violado y por lo tanto se contactó con su homónimo en el *Times* y compartió los cables. Los medios de comunicación al estar cansados de las constantes manipulaciones de Assange decidieron publicar un perfil del mismo, el *Times* lo nombró "El fundador de WikiLeaks a la fuga, perseguido por la fama" (Lundberg, 2011).

Las medidas tomadas comenzaron por campañas de desprestigio en contra de WikiLeaks, denominándolos una amenaza para la seguridad nacional. Autoridades del Ejército denunciaron las filtraciones como una violación a la confidencialidad de su inteligencia, lo que podría afectar sus operaciones en el extranjero y poner en grave peligro a quienes estaban a cargo de las operaciones, tal denuncia fue respaldada por diferentes grupos de derechos humanos como Amnistía Internacional (Carrasco, 2010).

Barack Obama (2010), en una rueda de prensa expresó su preocupación por las vidas y las operaciones de inteligencia en Afganistán, y asegura que son estas las críticas que durante su campaña hizo a la administración anterior. Es así que condujo una revisión a la política exterior y fortaleció su compromiso con la creación de una nueva estrategia de defensa integral que afronte estos problemas, así también la exigencia de una mayor rendición de cuentas por parte de sus socios en Afganistán y Pakistán.

Más tarde en el mismo año, se completó la revisión a la política del ciberespacio y se adoptó un plan de acción a corto plazo para abordar los problemas más desafiantes. Dicho plan se enfoca en el cambio e implementación de diferentes puestos de trabajo en ciberseguridad, así como campañas de concientización, colaboración con diferentes entidades públicas y privadas, y la creación de un plan de respuesta a incidentes (Department of Homeland Security, 2010).

En julio de 2011, el Departamento de Defensa formuló la Estrategia para Operar en el Ciberespacio con cinco iniciativas basadas, en primera instancia en concebir al ciberespacio como un dominio operacional a través del cual se pueda aprovechar el potencial de sus servicios. La segunda estrategia se refiere a la reformulación de los conceptos operacionales para una protección eficiente de los sistemas y redes nacionales. Por otra parte, las estrategias tres y cuatro están direccionadas a la cooperación, tanto nacional como internacional, respectivamente. Cabe recalcar que se hace un enfoque especial en las alianzas con otros departamentos y agencias, así como con el sector privado. En cuanto a las alianzas internacionales, se buscar reforzar aquellas ya existentes y establecer nuevas para redefinir la estrategia de seguridad y crear un concepto colectivo de la misma. Finalmente, la quinta estrategia busca tomar ventaja de la innovación tecnológica y un personal mejor capacitado para desarrollar el potencial nacional (Department of Defense, 2011).

La primera estrategia busca aprovechar el potencial que el ciberespacio proporciona. Por lo tanto, La Secretaría Nacional de Defensa asignó una comisión que opere en este dominio, conformada por el Comando Estratégico y departamentos militares. El *USCYBERCOM* se encargaría de gestionar las vulnerabilidades del ciberespacio (para los Estados)[13] con mayor capacitación a sus técnicos para crear redes seguras y resistentes y garantizar el desarrollo de las capacidades en conjunto. Además este comando se ocuparía de la sincronización

[13] Vulnerabilidades del Ciberespacio: Se hace referencia a las vulnerabilidades en la Tabla 1 del primer capítulo en “Los recursos del poder en el ciberespacio”.

y coordinación de las actividades entre la milicia, el Cibercomando de la Armada, de la Marina, Guardia Costera entre otros. Finalmente, se trabajaría con la NSA y bajo el comando de Comando Estratégico (Department of Defense, 2011).

La aplicación de nuevos conceptos de defensa para la protección de las redes y sistemas nace como una estrategia para actualizar procesos y que éstos se adapten a la naturaleza cambiante del ciberespacio. Se resalta la importancia de mantener un sistema que sea capaz de parar y mitigar las amenazas internas mediante la comunicación, rendición de cuentas monitoreo y manejo de las habilidades informáticas. La estrategia implementó un sistema de detección que prevenga las irrupciones en las redes nacionales a través de sensores, software e inteligencia. De esta manera también se invierte en el desarrollo e investigación de nuevas tecnologías que sean más eficientes de detección y mitigación de amenazas (Department of Defense, 2011).

La alianza con otros departamentos y agencias nacionales así como con el sector privado es una iniciativa que la aplicó el gobierno al entender que los nuevos desafíos del ciberespacio sobrepasan los esfuerzos del sector público. Las alianzas con proveedores de servicio de internet, el Departamento de Seguridad Nacional, FBI, CIA y NSA, así como con empresas privadas influyentes significaría crear una estrategia conjunto que beneficie a todos. En 2010, se firmó un memorándum aceptando la cooperación interagencia. Esto creará una estructura formal que establezca límites a las leyes y políticas, lo que a su vez permite incrementar la efectividad y proteger las libertades civiles y de difusión. De la misma manera, creó una alianza con la Base de Defensa Industrial para proteger la información confidencial tanto del gobierno como de las empresas, mientras entre sí comparten tecnologías sistemas y estrategias. Se decidió continuar con el programa lanzado en 2007 que promocione los beneficios de esta cooperación (Department of Defense, 2011).

Una vez cubiertas las necesidades nacionales, se pasó a la cuarta estrategia para afianzar las relaciones internacionales. El gobierno de los Estados Unidos

recalcó que es imperativo que el cibercrimen sea considerado como una amenaza mundial. Las acciones a tomarse con los aliados de Estados Unidos como Reino Unido, Canadá, Australia, Nueva Zelanda, entre otros, son intercambio de indicadores en tiempo real de cibereventos, así como el surgimiento de nuevos actores o amenazas. El Departamento de Defensa sería el encargado de manejar las operaciones de coordinación con los departamentos y las fuerzas militares de otros Estados (Department of Defense, 2011).

Finalmente, la quinta estrategia está basada en el desarrollo tecnológico que busca mejorar el personal técnico, científico y académico. Esta es una de las inversiones primordiales para que la innovación tecnológica se convierta en una ventaja para la nación. De esta manera se pretenden establecer programas que atraigan la participación de talento joven, así como programas de intercambio y capacitación constante. También se busca promover las oportunidades para empresas nuevas, pequeñas y medianas. Por lo tanto, el Departamento de Defensa es el encargado de desarrollar un *Cyber Range*, es decir, un modelo de redes que prueben y simulen las actividades en el ciberespacio en tiempo real, buscando vulnerabilidades y corrigiéndolas (Department of Defense, 2011).

2.2. Caso Snowden: nuevas filtraciones de la Agencia Nacional de Seguridad (NSA)

En 2013, Edward Snowden, ex contratista de la Agencia Nacional de Seguridad (NSA) y la Agencia Central de Inteligencia (CIA) accedió a los documentos de gobierno clasificados para filtrarlos a la prensa. Las filtraciones revelaban las operaciones de espionaje masivo de la NSA y la Agencia de Inteligencia Británica[14] con el objetivo de monitorear posibles ataques terroristas. Los datos se recolectaban directamente de cuentas de email, redes sociales, llamadas telefónicas, mensajes de textos, cámaras web con la ayuda de *Verizon*[15]

[14] GCHQ: Government Communications Headquarters
[15] Operador de telefonía móvil estadounidense, creada en el año 2000. Se constituye como la mayor operadora de este país (Verizon, s.F.).

y distintas compañías de internet como Google y Facebook bajo el programa PRISM[16] (THIBER, 2013).

Este apartado expone los documentos filtrados por Edward Snowden acerca de los programas de vigilancia y recolección de datos con el fin de detener el terrorismo. Por lo tanto, se analiza el marco jurídico que rige las operaciones de la Agencia Nacional de Seguridad (NSA) y las leyes que se aplican en contra de Snowden. Esta sección analiza de igual manera la eficiencia de las leyes y programas para procurar la seguridad post WikiLeaks, e identificar las fallas principales.

2.2.1. Documentos clasificados filtrados de la Agencia Nacional de Seguridad

Edward Snowden es un consultor tecnológico estadounidense nacido en Carolina del Norte, que prestaba sus servicios para la Agencia Central de Inteligencia (CIA) y la Agencia Nacional de Seguridad (NSA). Durante su adolescencia, Snowden tomó clases de computación en una universidad de Maryland, pero nunca terminó el curso necesario para obtener un diploma de bachiller. Durante este tiempo se dedicó a autoeducarse en Tecnologías de la Información (IT). En 2003, se unió al ejército de los Estados Unidos, no obstante tuvo un accidente durante los entrenamientos que lo inhabilitó a tener una participación activa. A pesar de no poseer un título, logró entrar en la CIA gracias a sus amplios conocimientos tecnológicos (Simcox, 2015).

En un principio, Snowden era simpatizante de la ideología del partido de George W. Bush, sin embargo durante su paso por la CIA descubrió que las actividades secretas del ex presidente revelaban una realidad diferente, que cambiaron su opinión. Las elecciones presidenciales del 2009 parecían ofrecer un cambio a las políticas represivas del gobierno anterior, puesto que el discurso de Barack Obama denotaba una clara oposición a su predecesor, lo cual hizo a Snowden repensar la filtración de información y esperar que el cambio de

[16] Programa de vigilancia bajo el cual la NSA recolecta comunicaciones en el ciberespacio.

presidencia solucione estos problemas. Para su desilusión, Obama continuó con las prácticas de Bush, a pesar de que lo hacía de manera sutil y discreta (Simcox, 2015).

Cronología de las revelaciones

En 2009, decidió abandonar la CIA después de su participación diplomática en Ginebra, la cual terminó debido a la comprobación del espionaje que realizaba Estados Unidos al mundo entero; y comenzó a trabajar para la NSA a través de la compañía Booz Allen Hamilton[17], con el objetivo de recabar información relevante para su posterior revelación. Snowden fue asignado a un proyecto en Hawaii, donde corroboró finalmente todos los programas de espionaje y su verdadero objetivo (Simcox, 2015).

> En 2013, dejó su vida en Hawaii para viajar a Hong Kong a encontrarse con periodistas, Glenn Greenwald, Laura Poitras y Ewen Macaskil de *The Guardian* y *The Washington Post.* Durante la reunión secreta, en una habitación de hotel, Edward Snowden reveló sus razones para la filtración de información y entregó un *pen drive* con todos los documentos clasificados para su posterior publicación en los periódicos previamente mencionados (López, 2014).

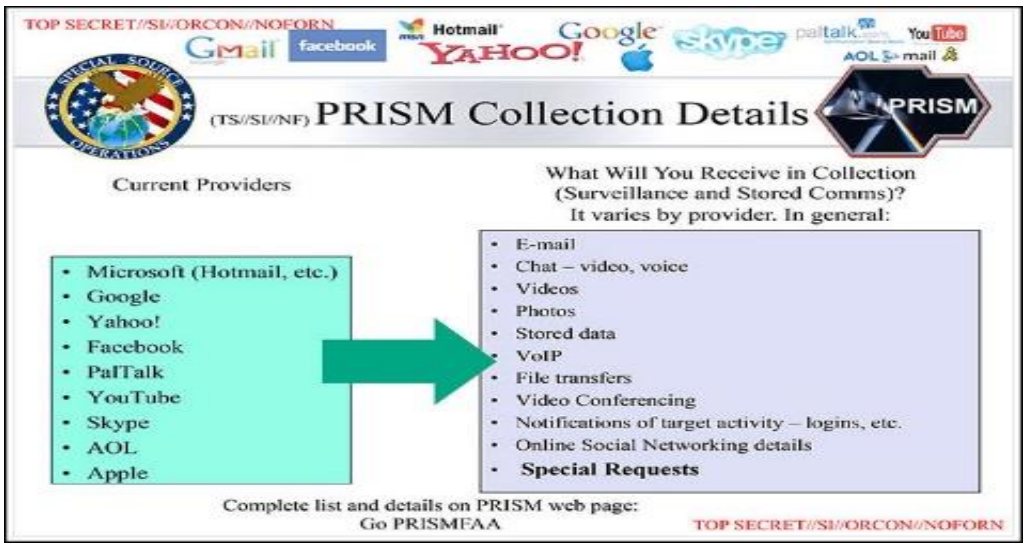
El 5 de junio. La circulación de información inició en el periódico *The Guardian*, y trató acerca de la recolección masiva de registros de llamadas telefónicas de la compañía Verizon[18] (López, 2014).

El 6 de junio. Se revela el programa PRISM, que era la herramienta principal de la NSA para recolectar datos electrónicos de cuentas de correo de Gmail, Outlook e incluso Facebook; de la misma manera tenían autorización de Google, Yahoo! y Apple para solicitar información específica de personas de interés. Esto se puede evidenciar en la Imagen 1, que puntualizan los proveedores, en la primera columna, y en la segunda los lugares de dónde provenía la información. La creación de este programa fue una medida tomada después del

[17] Empresa de consultoría estadounidense de tecnología y seguridad (Booz Allen, s.F.)
[18] Compañía de telefonía estadounidense que abarca el 90% de servicio

ataque terrorista del 2001, y se lo manejó con la clasificación de “secreto” como un plan de vigilancia del terrorismo (López, 2014). Posteriormente, la NSA desclasificó los documentos referentes al programa, corroborando la información proveniente de Snowden (NSA, s.f.).

IMAGEN 1
DETALLES RECOLECCIÓN DE DATOS *PRISM*



Fuente y Elaboración: (NSA, s.f.)

El 9 de junio. Se publica la entrevista realizada a Snowden, revelando la identidad del responsable de la extracción de información. Entre el 11 y 30 de junio se revela el espionaje a China, Rusia, Alemania, entre otros. De la misma manera se da a conocer que la *CGQH*, agencia británica de inteligencia, colaboraba con Estados Unidos y se transfería información confidencial de ciudadanos estadounidenses y británicos. De la misma manera se descubre que Francia y Australia aportaban con información y que Estados Unidos investigaba a las embajadas de otros países (López, 2014).

Las tácticas de la NSA

Las revelaciones dieron a conocer que la NSA recibía órdenes directas de la Casa Blanca para rastrear posibles criminales y, mediante su programa de recolección de datos masivos en países extranjeros se procedía a su localización y

dependiendo del riesgo, se realizaban detenciones o ataques. El programa consistía en detectar a potenciales criminales basados en un análisis tecnológico de la información proporcionada por el espionaje a las comunicaciones, para después localizar el teléfono. Posteriormente y sin un análisis humano, se pedía a la CIA o a las fuerzas militares atacar el lugar de donde provenía la señal. Estas declaraciones fueron corroboradas por un ex operador de drones para el Comando Conjunto de Operaciones Especiales[19] que decidió permanecer en el anonimato; de la misma manera, el ex operador de sensores de drones de la fuerza aérea, Brandon Bryant, confirmó y criticó las operaciones letales que se llevaban a cabo en Irak, Afganistán y Yemen. Sin el análisis humano que compruebe la identidad de los terroristas o criminales, que se encuentran conscientes de la geolocalización de la NSA, es altamente probable cometer errores y tener muertes colaterales (Greenwald, 2014).

Las tácticas de la NSA, no solo se basan en el ataque y detención de terroristas, sino que infiltran agentes en internet para manipular y controlar los discursos mediante engaños y destrucción de reputaciones. Agencias que forman parte de "Five eyes"[20], utilizan las mismas herramientas que los hackers y criminales, a los que pretenden derrotar, como ataques DDoS[21], *honey traps*[22] o virus destructivos. Además filtran información falsa en internet acerca de personas o empresas que han criticado o expuesto sus prácticas, con la intención de desacreditarlos. Una táctica muy común es la publicación de artículos científicos que manipulan la opinión pública (Greenwald G. , 2014).

Los documentos clasificados revelaron también que la NSA desarrolló tecnología que infectaría con *malware* a millones de computadoras en todo el mundo, lo cual permitirá irrumpir en los ordenadores y extraer información

[19] JSOC, por sus siglas en inglés o Joint Special Operations Command
[20] La alianza de los "Cinco Ojos" es una alianza secreta de vigilancia global conformada por la NSA, la GCHQ de Reino Unido, Establecimiento de Seguridad de Comunicaciones de Canadá (CSEC), la Dirección de Señales Australianas y el Buró de Seguridad de Comunicaciones del Gobierno de Nueva Zelanda (GCSB) (Privacy International, s.f.).
[21] Ataques de Denegación de Servicios
[22] Práctica investigativa que tiene un propósito político, monetario o interpersonal, utilizando las relaciones románticas o sexuales como forma de extorsión.

relevante de redes extranjeras de Internet y comunicaciones por teléfono. El programa XKeyscore permite hacer una búsqueda similar a Google, que con palabras claves buscará las conversaciones que coincidan. Este sería usado a favor de Estados Unidos en sus sedes en Maryland, así como en Reino Unido y Japón. La manera de introducirse sería a través de servidores falsos de redes sociales como Facebook, envío de spams y mails que permiten el acceso al micrófono o a la cámara web. Estas operaciones se llevarían a cabo para realizar ciberataques a sitios web de interés (Gallagher, 2014).

2.2.2. Marco Jurídico de la NSA y la legislación internacional pertinente al caso Snowden

Snowden viajó de Hawái a Hong Kong después de robar la información clasificada a la NSA, se reunió con periodistas y escritores encargados de difundir los documentos. El 21 de junio, 2013, después de revelada su identidad, Estados Unidos presentó cargos de espionaje en su contra y pidió a la República Popular de China la extradición después de presentar las pruebas pertinentes. El gobierno chino denegó la petición alegando insuficiencia de pruebas, lo cual permitió a Snowden escapar. Después de asesorarse con los empleados de WikiLeaks y abogados, fijó su destino a Ecuador para pedir asilo, sin embargo entre su viaje de Hong Kong a Moscú, el gobierno estadounidense revocó su pasaporte. Esto provocó su permanencia en la zona de tránsito del aeropuerto, en el que residió varios días hasta pensar su próximo paso. Finalmente, realizó una aplicación de asilo en Rusia la cual fue aceptada por un año, y más tarde extendida. Hasta el presente, Snowden permanece en la ciudad de Moscú como residente legal hasta 2020 (Simcox, 2015).

Snowden dice no ser un traidor a su patria, al contrario su interés está en incentivar el desarrollo y progreso de la tecnología de Estados Unidos, pero así también una crítica a las acciones tomadas por los gobiernos, destinadas a la violación de derechos civiles. Snowden alegó que no regresara a Estados Unidos pues está seguro que sus derechos no serán respetados y no tendrá un juicio público ni justo. Sus argumentos principales están basados en el hecho que las

leyes que se establecieron para regular a las agencias e instituciones nacionales, se las utiliza en contra de los ciudadanos. Este es el caso de la Ley de Espionaje, *Patriot Act* y FISA (Simcox, 2015).

Ley de Espionaje

Los cargos que enfrenta Snowden están regidos bajo el marco de la Ley de Espionaje de 1917, la cual protege la información nacional en cuanto a estrategias de defensa, así como secciones especiales dedicadas a los funcionarios o trabajadores que tienen acceso a información clasificada. El espionaje está catalogado como traición, lo cual aplicaría solo para aquellos que deben lealtad a Estados Unidos. En el código 18 de este país, sección 793 establece la prohibición de la recolección, transmisión y recepción de información de defensa con el fin de utilizarla en contra del país o en beneficio de otro Estado. Por lo tanto, cualquiera que intencionalmente viole esta ley deberá ser multado, no más de diez años de prisión, o ambas penalizaciones. La sección 1924 establece la prohibición de posesión no autorizada de información clasificada, así como la sustracción de material por parte de los empleados de gobierno, contratistas o consultores, que adquieran dicha información mediante los privilegios otorgados por su trabajo. Su multa será de no más de $1000 y el máximo de un año de prisión (Yoon, 2015).

Patriot Act

El Patriot Act es una ley que permite al gobierno estadounidense recopilar metadatos de telefonía, es decir fecha, hora, duración y número remitente y destinatario. El proceso se lleva a cabo gracias a los servidores de comunicación y que se encuentran en una caja de seguridad virtual de la NSA. La agencia, al tener una sospecha razonable de actividades terroristas, puede acceder a los metadatos. En la sección 215 se establece que se ayudará a las agencias gubernamentales a realizar conexiones entre las comunicaciones para detectar posibles planes terroristas. Su mayor ventaja se presentaría al detectar de manera temprana dichos planes (Simcox, 2015).

FISA: Ley de Vigilancia Extranjera

Dentro del *Patriot Act*, el gobierno de Estados Unidos está regido bajo las leyes *FISA*, por sus siglas en inglés *Foreign Intelligence Surveillance Act*, o Ley de Vigilancia de Inteligencia Extranjera, para afirmar sus acciones en cuanto al espionaje internacional llevado a cabo con el fin de detener el terrorismo (Herrington, 2015).

La sección 702 de FISA establece que se puede interceptar las comunicaciones de los ciudadanos extranjeros que se encuentras radicados fuera de Estados Unidos, con el fin de extraer información de inteligencia para la seguridad nacional con enfoque especial en terrorismo, espionaje y armas de destrucción masivas. Esta sección permite al gobierno adquirir la información mediante proveedores de servicios como Google, Yahoo!, Microsoft, Facebook y Apple, entre otros, consintiendo su acceso a conversaciones telefónicas y correos electrónicos. Esta es la herramienta más importante para la NSA en cuanto a detección, identificación y detención de amenazas terroristas a nivel mundial, con enfoque especial en su nación (Simcox, 2015).

FISA tiene sus orígenes en el Programa de Vigilancia del Terrorismo, creado después de los ataques de Al Qaeda contra Estados Unidos en el 9/11. Los registros se obtenían bajo autorización presidencial que demostraba la existencia de una emergencia por una amenaza terrorista; el programa permitió la exclusión de una orden judicial. Después de 2007, el Tribunal de Vigilancia de Inteligencia Extranjera (FISC) era el encargado de autorizar dichas actividades, siempre y cuando existiera causa probable; esto dificultó las operaciones y condujo a una reformulación de la ley en agosto del 2007, donde se eliminó la necesidad de que el gobierno solicite órdenes judiciales individuales si en las evidencias se proporcionaban indicios de terrorismo. Para esto existen dos programas de adquisición de datos: *PRISM* y *Upstream*[23] (Simcox, 2015).

[23] Colección *Upstream* hace referencia a la intervención de la NSA en las redes de cable de fibra óptica subacuática o red troncal de internet donde convergen datos de teléfono e internet tanto dentro y fuera de Estados Unidos.

Convención de Budapest o Convención sobre Cibercrimen

Dado que el mundo es interdependiente, dentro del ámbito internacional, existe la necesidad de crear cooperación y tratados que legislen el ciberespacio. Los dos tratados más relevantes en el caso de Snowden son: la Convención de Budapest y la Unión Internacional de Telecomunicaciones (ITU por sus siglas en inglés)[24].

La Convención de Budapest, la cual se realizó el 23 de noviembre del 2001, es el primer tratado internacional sobre el ciberespacio que busca definir y aplicar una política penal que proteja a los ciudadanos de los crímenes presentes en este dominio, mediante la cooperación. Además, es el único tratado vinculante sobre este tema, el cual busca ser una guía para el desarrollo de una legislación de cada Estado miembro. El tratado establece normas generales acerca de los derechos de autor, fraude informático, pornografía infantil, y violaciones de seguridad dentro de las redes informáticas (Convención de Budapest, 2001).

El objetivo es que se definan los tipos de conducta que son calificados como delitos, es decir, acciones que atenten contra la confidencialidad, integridad y disponibilidad mediante el uso de sistemas informáticos. De esta manera, el siguiente paso planteado es el de proporcionar un medio efectivo para que la justicia penal aborde los temas y aplique las herramientas necesarias de detección e investigación. Sin embargo, estas recomendaciones son generales con el objetivo de que los Estados apliquen condiciones y salvaguardias que limiten e impidan el abuso de poder y protejan, por sobre todo, los derechos humanos. Finalmente, se insta a los Estados miembros a participar en la cooperación internacional (Seger, 2012).

[24] International Telecommunication Union

ITU (International Telecommunication Union)

Es un organismo de la Organización de las Naciones Unidas que se encarga de regular las telecomunicaciones internacionales. Su objetivo principal es proteger y respaldar el derecho a una comunicación libre, la cual a través de la tecnología se realiza con mayor facilidad. Tiene 193 países miembros y trabajan conjuntamente con expertos en el ciberespacio para la creación de leyes y reglas de convivencia. La organización está convencida de que al aplicar leyes, se genera confianza entre los miembros, además facilita el desarrollo e implementación tecnológica (UIT, s/f).

En la Resolución 130, de 2014 se enumeran y reconocen amenazas y tendencias nuevas dentro de este dominio, siempre enfatizando la necesidad de mejorar la cooperación y el desarrollo de políticas nacionales, regionales e internacionales. La principal preocupación de este organismo es la erosión del control nacional frente a actores no estatales dentro del ciberespacio, puesto que las ventajas que promueve el internet hace más fácil la tarea de grupos o individuos terroristas que tratan de irrumpir la paz cibernética (UIT, 2014).

2.2.3. Las violaciones al marco jurídico que rige la vigilancia masiva

La NSA, respaldado por el *Patriot Act* y FISA, ha recopilado la información de personas de interés, lo cual es permitido como medida para detener el terrorismo o cualquier crimen que puede ocurrir en contra de la seguridad nacional e internacional. Sin embargo, las filtraciones de Edward Snowden revelan una realidad diferente, pues las comunicaciones de los ciudadanos estadounidenses, que son tomadas de manera accidental se almacenaban en sus bases de datos. Por otro lado, también se dio a conocer que la recolección de información se realizó sin presentar causa probable para analizar a un individuo específico, sino que se hizo de manera general, lo cual está considerado como una violación a la constitución, establecida bajo la Sección 702. No obstante, se llegó a la conclusión que la petición fue autorizada por el Congreso, que según la Cuarta

Enmienda[25] tiene la potestad de realizarlo y se la consideró una herramienta efectiva y válida (Simcox, 2015).

Debido a la toma ilegal de las comunicaciones, la NSA ha violado las reglas de privacidad 2776 veces entre abril del 2011 y marzo del 2012. A pesar de estos descubrimientos, la agencia no fue sancionada pues se falló a favor de la misma debido a las medidas que se tomaron de manera posterior al descubrimiento del problema. La NSA borró toda información concerniente a la recolección accidental de datos y argumentó que esta actúa de buena voluntad, pero que existen todavía errores presentes en sus programas que están tratando de ser solucionados. Benjamin Wittes[26] (2014) dijo que "el proceso no es perfecto, pero tiene integridad". En 2011, se detectó problemas tecnológicos dado que se estaba reteniendo demasiada información innecesaria y resultaba en el almacenamiento ilegal de información (Simcox, 2015).

El conflicto y la razón por la que Edward Snowden decide filtrar la información y permitir que se sepa la verdad se dirigiría a la manera de actuación del FISC. Cabe recalcar que la corte solo acepta pedidos de espionaje una vez presentadas las evidencias de un posible ataque o crimen, pero al ser actividades clasificadas como secretas, el tribunal organiza reuniones secretas con representantes gubernamentales, cerradas al público y sus decisiones están archivadas de manera clasificada. Durante esta reunión, se procede a realizar preguntas acerca de la petición, pero no existe una argumentación adversa. Entre 1979 y 2012, se realizaron más de 30 000 peticiones, de las cuales solo 11 fueron rechazadas, es decir un 0,032%. De la misma manera, las funciones de la corte han sido progresivamente ampliadas de acuerdo a las necesidades del gobierno, por lo que en 2008, esta ha sido concedida procedimientos cuasi constitucionales que protegen, con carácter retroactivo, a aquellas compañías de servicios telefónicos que proveen información de manera ilegal y convirtiendo a estos

[25] La cuarta enmienda de la Constitución de los Estados Unidos protege dos derechos fundamentales: el derecho a la privacidad y el derecho a no sufrir una invasión arbitraria (Constitución de los Estados Unidos, s.f.).
[26] Periodista e investigador estadounidense experto en temas de seguridad nacional y leyes.

programas de vigilancia como parte de los poderes constitucionales del gobierno (O'Neill, 2014).

Otra de la razones se basa en la interpretación de la ley, que deja un amplio espectro para la interpretación, puesto que la Sección 702 está enfocada hacia las pautas marcadas para la vigilancia de objetivos extranjeros. Estas características han permitido espiar las comunicaciones de los ciudadanos estadounidenses. El programa examina las comunicaciones del objetivo planteado y amplía su búsqueda a sus contactos y los contactos de sus contactos, incluso si estos son inocentes. Por lo tanto, la red mundial de internet tiene una puerta trasera que conduce a los servidores la NSA, pero la corte FISA no regula los procedimientos de la Sección 702, pues el tribunal los aprueba en el plazo de un año, es decir que existe una falta de supervisión judicial. De la misma manera, el Congreso tampoco está al tanto de estas actividades (Kayyali, 2014).

2.3. Las repercusiones de las filtraciones en la política de ciberdefensa

El gobierno de Barack Obama y la imagen de Estados Unidos en el mundo se vieron afectadas debido a las filtraciones. En primera instancia, la credibilidad, influencia y legitimidad que Obama recuperó en sus primeros años de mandato, sufrieron graves consecuencias, pues dejaron en evidencia los verdaderos intereses de Estados Unidos; esto es la necesidad de control a pesar de reflejar tintes autoritarios que violan los derechos humanos (Lewis, 2014). La opinión pública reveló la preocupación por los programas anti terroristas, que invaden su privacidad y siguen siendo insuficientes para protegerlos o están mal direccionados (Rainie, 2016).

Las filtraciones detectaron los graves problemas de seguridad que tiene la agencia, por lo tanto se tomaron medidas enfocadas en reformar la misma, en especial ocultar los documentos clasificados para que analistas no puedan acceder a los mismos (NPR, 2013). Por otro lado, Obama aseguró que la crisis en la que se encuentra Estados Unidos debido a las revelaciones crea una oportunidad de

debatir acerca de las leyes de privacidad, lo cual finalizó en la reformulación de la Ley de Espionaje en 2015 (ANSA y DPA, 2015). De la misma manera, se creó el Centro de Recolección de Información de la NSA en Utah y se trabajó en la transparencia de la agencia al publicar los documentos revelados por Snowden (NSA, 2014).

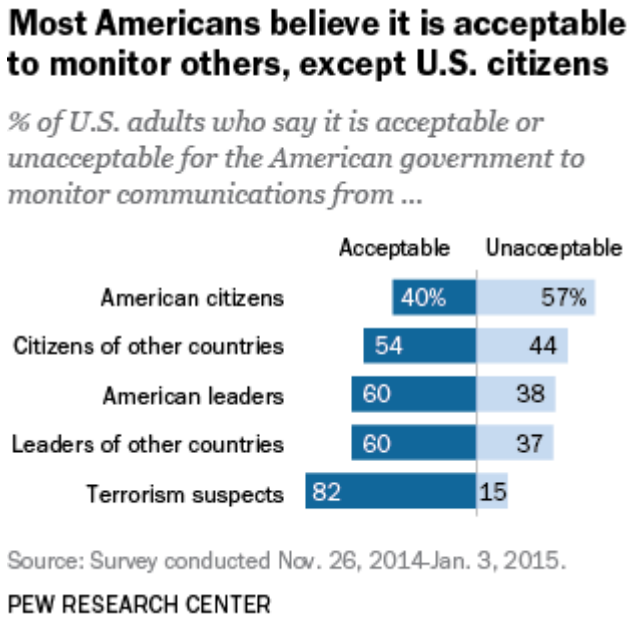
Finalmente, esta sección analiza las repercusiones de las filtraciones, comenzando por un análisis de la confianza en el gobierno de Obama antes y después de las filtraciones, tanto nacional como internacionalmente. Se continuará con un análisis de las repercusiones legales y los cambios realizados para mantener la calma en la sociedad. Finalmente, se explicarán las medidas tomadas en cuanto a la Agencia Nacional de Seguridad y sus programas de vigilancia y recolección de datos que incluirían mejorar la infraestructura, reformar sus leyes internas y aumentar la transparencia.

2.3.1. La opinión pública nacional e internacional sobre las violaciones de privacidad

Opinión pública nacional

En el 2009, al inicio del nuevo periodo presidencial, Obama contaba con el apoyo del 74% de la población, que confiaban en que el nuevo presidente tomaría las decisiones correctas. En 2014, Obama continua manteniendo esa confianza excepto en los países de Medio Oriente. A pesar de las filtraciones de información, el 58% de la población nacional continúa confiando en su gobierno (Pew Research Center, 2014). Sin embargo, se constata una desaprobación frente a los programas de monitoreo de sus comunicaciones. De esta manera, en una encuesta realizada a la población estadounidense en los años 2014 – 2015 muestra que el 57% de los ciudadanos piensa que el monitoreo es inaceptable (Gráfico 3). Por otro lado, el 60% de los líderes estadounidenses, piensa que son aceptables las medidas tomadas por el gobierno (Rainie, 2016).

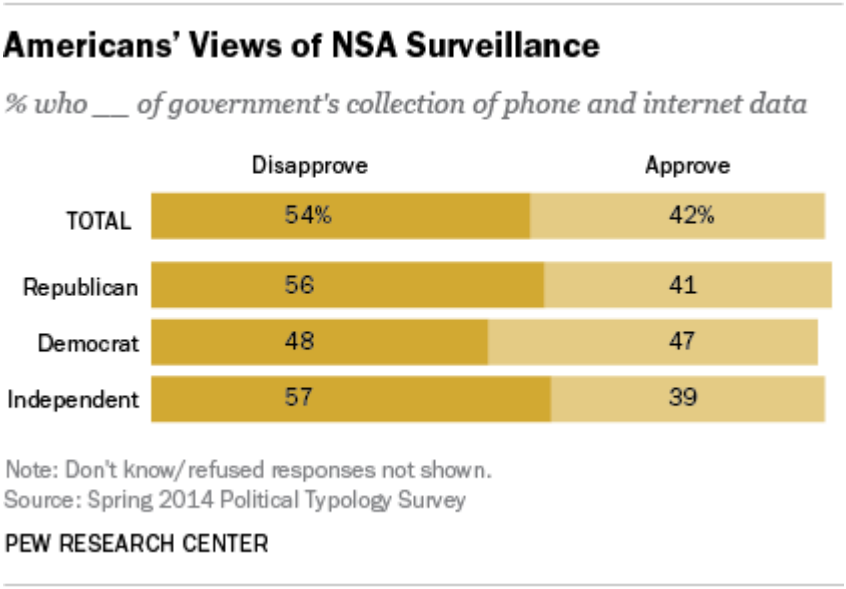
GRÁFICO 3
PORCENTAJE DE ACEPTACIÓN DE LOS PROGRAMAS DE VIGILANCIA



Fuente y Elaboración: (Pew Research Center, 2014)

En cuanto a las operaciones que realiza la NSA, en otra encuesta dirigida en 2014 – 2015 se muestra que el 54% de los ciudadanos desaprueba recolección de datos de teléfonos e internet (Gráfico 4). Los republicanos la desaprueban en un 56%, mientras que los demócratas un 48% y los independientes un 57%. Los ciudadanos piensan que no existe la necesidad de sacrificar su privacidad y libertades civiles para estar a salvo del terrorismo. Por el contrario, están convencidos que mejores y más rigurosas políticas podrían ayudar a detener el terrorismo, el 49% está de acuerdo en que el gobierno no ha establecido políticas anti terrorismo efectivas (Gao, 2015).

GRÁFICO 4
PORCENTAJE DE APROBACIÓN NACIONAL FRENTE A LOS PROGRAMAS DE VIGILANCIA

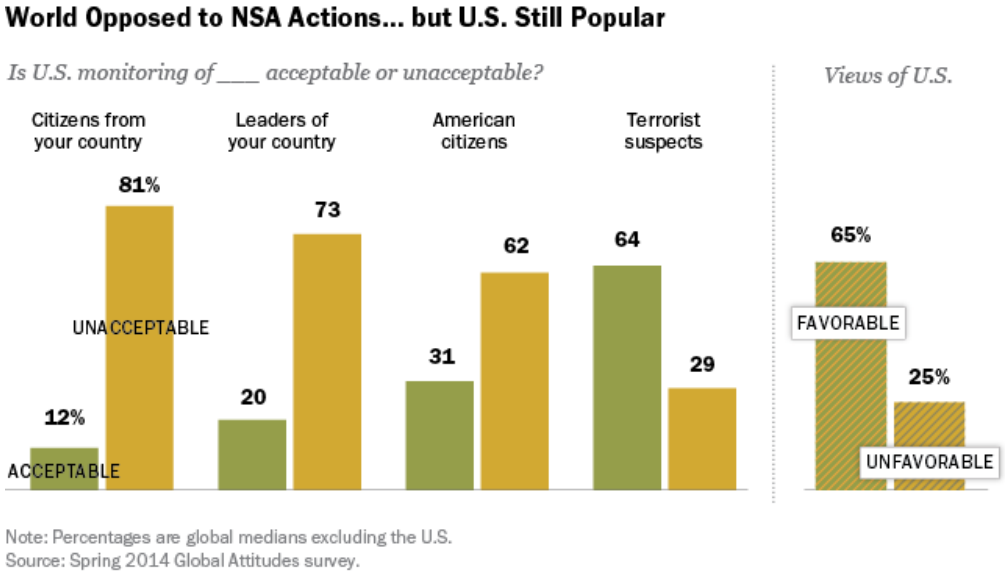


Fuente y Elaboración: (Pew Research Center, 2015)

Opinión Pública Internacional

En cuanto a la opinión pública y líderes internacionales, en una encuesta realizada en 2014 sobre las acciones de la NSA para asegurar su territorio frente a los ataques terroristas, podemos observar en el gráfico 5 que el 81% de los ciudadanos de distintos países no está de acuerdo con que Estados Unidos monitoree sus comunicaciones. Solo el 20% de los líderes mundiales aprueba estas acciones. A pesar de no consentir los programas, el 65% percibe de manera favorable a Estados Unidos. La oposición a los programas está dirigido principalmente al uso de drones para ataques aéreos a extremistas, el 68% en promedio de los países encuestados se opone al uso de drones (Pew Research Center, 2014).

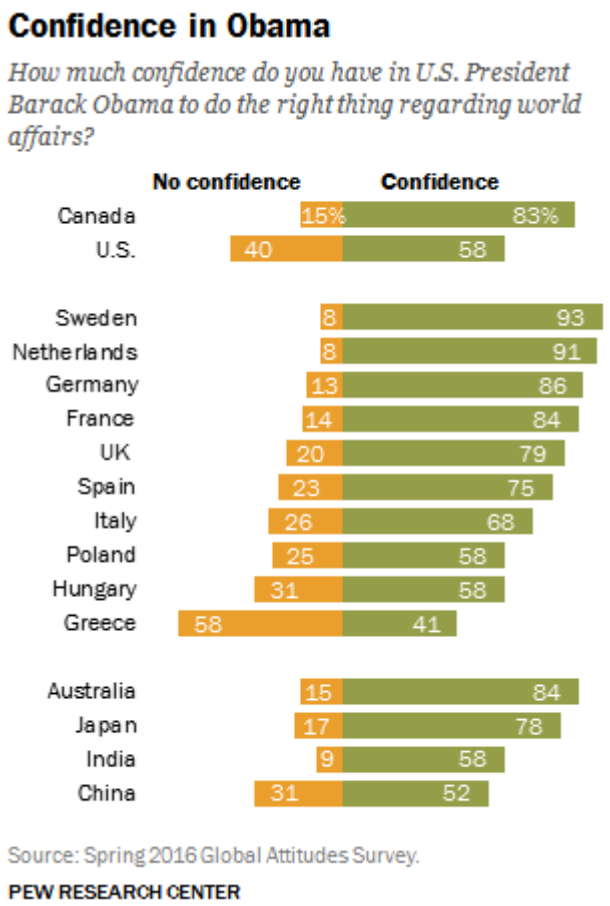
GRÁFICO 5
PORCENTAJE DE ACEPTACIÓN DE LO PROGRAMAS DE LA NSA Y POPULARIDAD DE ESTADOS UNIDOS



Fuente y Elaboración: (Pew Research Center, 2014)

Dentro de otra encuesta, realizada en 2016 sobre la confianza que los ciudadanos estadounidenses y de otros países tienen en la administración de Obama, la mayoría muestra una gran acogida a la política exterior y su habilidad de manejar los asuntos internacionales. En el gráfico 6, podemos observar que la mayoría de países encuestados confían en esta administración, a excepción de Grecia y China, los cuales presentan un 58% y 31% respectivamente de desconfianza en el gobierno del presidente número 44 de los Estados Unidos (Poushter, 2016).

GRÁFICO 6
PORCENTAJE INTERNACIONAL DE CONFIANZA EN OBAMA



Fuente y Elaboración: (Pew Research, 2016)

El efecto Snowden, es el fenómeno que erosionó la fe del mundo en Estados Unidos para proteger y respetar sus libertades personales. Entre 2013 y 2014 la confianza en Estados Unidos bajó aproximadamente un 14,50%, aun así individualmente la totalidad de países encuestados presenta más del 50% de confianza en este país, a excepción de países de Medio Oriente. Por esta razón, Bangladesh, India, Indonesia, Japón, Filipinas, Reino Unido entre otros considera como su mayor aliado a Estados Unidos (Pew Research Center, 2014).

GRÁFICO 7
CONFIANZA EN LA PROTECCIÓN DE LAS LIBERTADES PERSONALES EN LOS ESTADOS UNIDOS

Eroding Faith in Protection of Personal Freedoms in the U.S.

U.S. gov't respects personal freedoms

	2013 %	2014 %	Change
El Salvador	79	50	-29
Brazil	76	51	-25
Germany	81	58	-23
Pakistan	54	31	-23
Argentina	54	32	-22
Russia	67	47	-20
South Africa	70	52	-18
Nigeria	70	53	-17
Mexico	55	38	-17
Greece	58	43	-15
Chile	66	53	-13
Malaysia	63	50	-13
Spain	69	57	-12
France	80	69	-11
UK	75	65	-10
Uganda	70	60	-10
Senegal	72	63	-9
Israel	83	75	-8
Italy	82	75	-7
Indonesia	69	63	-6
U.S.	69	63	-6
Palest. ter.	66	60	-6

Only statistically significant changes shown.

Source: Spring 2014 Global Attitudes survey. Q109b.

PEW RESEARCH CENTER

Fuente y Elaboración: (Pew Research Center, 2014)

En cuanto a la percepción de la protección a las libertades personales, los países encuestados, los cuales representan a diferentes partes del mundo, entre 2013 y 2014, el porcentaje de fe que tienen en Estados Unidos disminuyó entre 6% y 30%. Sin embargo, la imagen de Estados Unidos y la confianza depositada en el mismo no varían, puesto que sus acciones se ven justificadas debido a los constantes ciberataques terroristas (Pew Research Center, 2014).

2.3.2. Reformulación legal: Ley de Ciberseguridad

El gobierno de Barack Obama tuvo que proceder de manera diferente frente a las filtraciones de Snowden, lo cual lo llevó a reformular las leyes que rigen las operaciones y programas de la NSA, así como cambios en la manera de proceder respecto a la transparencia y los problemas de seguridad que se evidenciaron al permitir que un contratista externo robara y filtrara información clasificada. El Departamento de Defensa señaló que ciertas técnicas de recolección de datos tendrían que cambiar su funcionamiento o detenerse por temor a que los criminales detecten sus métodos y bloqueen sus señales (Simcox, 2015).

Este es el caso de China y Rusia, que adoptaron esta metodología de recolección de información y detectaron los puntos débiles en la infraestructura de Estados Unidos y Reino Unido y las usaron en su contra. De la misma manera, en 2015 un video jihadista advertía a sus seguidores la manera de estar protegidos frente al espionaje, dado que al estar en contacto con las torres de señal se puede acceder al historial diario de una persona. También daba una lista de software que puede ser instalado en el instrumento de comunicación para lograr no ser detectado y donde se pueden comprar (Simcox, 2015).

Snowden declaró que su interés siempre fue el bienestar de Estados Unidos, debido que piensa que las capacidades de ese país son superiores a los resultados que se obtiene. Según Snowden, él dejó varios indicios que llevarían al servicio de inteligencia a descubrir exactamente los documentos que robó; sin embargo, afirmó que las declaraciones de los dirigentes del Departamento de Defensa acerca de la cantidad de información filtrada excede la cifra real, lo que lo lleva a pensar que no pudieron seguir sus pistas y por lo tanto, demuestra la deficiencia de la inteligencia estadounidense (Kirk, 2014).

Las políticas relacionadas con la vigilancia se fortalecieron, e incluso se crearon nuevas leyes que rijan estas acciones. Es el caso del *Freedom Act* que, a mediados de 2015 fue aprobada la ley que regulará y controlará el espionaje de la

NSA, en especial se centra en la recopilación masiva de metadatos, en la terminación de las leyes secretas del FISC y la introducción de un defensor de asuntos públicos y privacidad (Reitman, 2015). Entre las cláusulas que fueron admitidas están la necesidad de requerir más documentos a las autoridades de FISA para realizar sus operaciones de espionaje. Se le concede mayor oportunidad a las compañías de servicios de informar sobre los pedidos de la NSA, y desclasifica los resultados de la FISC o un resumen de los procesos judiciales. Aumenta la pena máxima de 15 a 20 años a aquellos que apoyen el terrorismo (The Washington Post, 2015).

Existe un aspecto rescatable de las filtraciones, y es el hecho que el sector privado, en especial las compañías de servicios telefónicos e internet que proporcionaban información al gobierno, lanzaron una Coalición para reformar la vigilancia que realizan los gobiernos a sus ciudadanos. De la misma manera, las empresas han empezado a mejorar sus sistemas de encriptación y hacer mayor énfasis en su privacidad, y ofrecer estos servicios a sus clientes. Finalmente, los individuos empiezan a tomar las mismas acciones para proteger su privacidad y mejorar sus habilidades tecnológicas en contra del espionaje (Amnistía Internacional, 2015).

Ley de Intercambio de Información de Ciberseguridad

La Ley de Ciberseguridad fue establecida el 18 de diciembre del 2015 para que el Departamento de Seguridad Interna, en colaboración con agencias nacionales, cree un proceso de intercambio de información voluntario que promueva la protección entre los miembros tanto privados como ciudadanos, y entre los mismos compartan tácticas y procedimientos para contrarrestar las amenazas cibernéticas. Debido a las filtraciones de la NSA, el documento promueve la protección de los derechos civiles y de privacidad (Department of Homeland Security, 2015).

La Orden Ejecutiva 13691, establecida en febrero del mismo año señaló loas antecedentes de la Ley de Seguridad. La orden promueve el intercambio de

información como medida para eliminar las amenazas cibernéticas y colaborar de manera conjunta al momento de respuesta. De la misma manera se establece que estas alianzas ayudaran a determinar mecanismos que mejoren las capacidades y funciones con miras a la protección de la privacidad, confidencialidad y salvaguardando la información compartida. Finalmente establece que es necesaria la formación de un grupo de Organizaciones de Análisis e Intercambios de Información conformados por el sector público y privado, para determinar las funciones de cada actor (The White House, 2015).

2.3.3. Reestructuración de la Agencia Nacional de Seguridad

A fin de evitar las críticas que empezaban a surgir por parte de líderes mundiales como Dilma Rousseff, que describió las acciones de la NSA como una violación a los derechos humanos y a las libertades civiles, se empezó a proponer una serie de reformas. El presidente Obama nombró un grupo de expertos que examinen los problemas presentes, el cual recomendó más de 40 reformas entre las cuales se mencionaba la finalización de los programas de recolección de información masiva y el espionaje a líderes políticos extranjeros. Del mismo modo, se aconsejó que sean los proveedores de servicios de internet y telefónicos aquellos que almacenen los metadatos (Byman, 2014).

En un discurso presidencial, Obama defendió a la agencia argumentando la necesidad de los programas para la seguridad nacional y aseguró que ninguna acción se ha llevado a cabo con el fin de violar la ley o los derechos ciudadanos. Así también restringió las actividades de la NSA para la obtención de información de objetivos específicos, la cual deberá conseguir una orden del FISC y solo se podrá analizar a las personas con las que habla directamente el objetivo principal. Finalmente, aseguró que abría una época de transición para terminar con la recolección de datos, y por lo tanto, dos meses después se anunció que las compañías telefónicas serían las responsables de almacenar los metadatos (Byman, 2014).

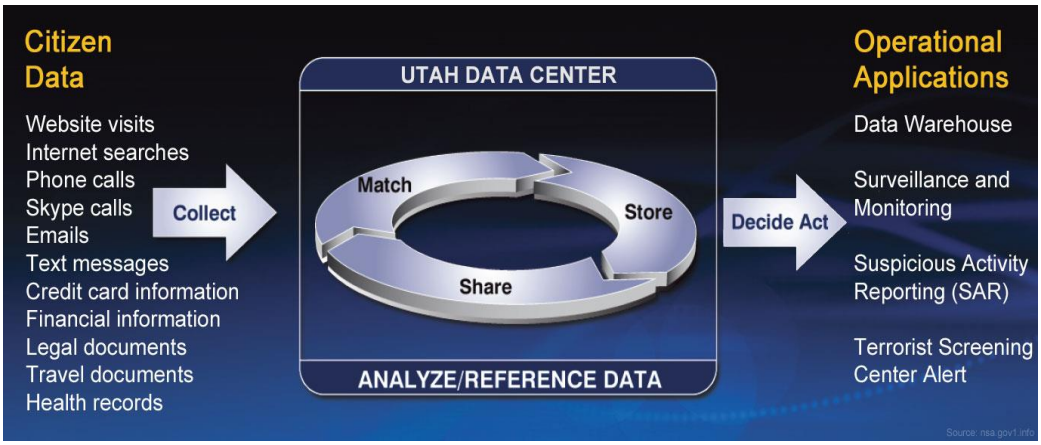
Sin embargo, se señaló que Estados Unidos espiará a ciudadanos no estadounidenses y a líderes mundiales si existe un motivo válido para los propósitos de seguridad. Lo que realmente preocupa a los ciudadanos es la deficiencia en cuanto a la defensa puesto que el gobierno ha visto disminuida su capacidad de mantener sus secretos y la falta de transparencia al hacerlo (Byman, 2014).

La agencia comenzó por crear un centro de datos en Utah, llamado Bumblehive, que asistirá en los esfuerzos de la Comunidad de Inteligencia de monitorear, fortalecer y proteger la infraestructura digital y física de Estados Unidos. Este centro está planeado como una unidad de almacenamiento masivo que soportaría la cantidad de información digital que se recolecta día a día. Las instalaciones costaron aproximadamente 1 500 millones de dólares y cuenta con 20 edificios totalmente equipados para asegurar la explotación del 100% de la capacidad. Según Gary R. Herbert (2012), gobernador de Utah, esta será la primera instalación en almacenar un yottabyte[27]. Habrá un aumento constante de las computadoras y desarrollo de plataformas digitales que mantendrán el paso acelerado del progreso de la tecnología (NSA, 2014).

Finalmente, la agencia decidió revelar sus tácticas de obtención de información en el nuevo centro, la cual se presenta en la Imagen 2. Se recolectará información de visitas a sitios web, búsquedas en internet, llamadas telefónicas, Skype, email, información bancaria, legal y salud que será analizada, compartida y almacenada para definir las acciones a tomar y bajo qué aplicación operativa será procesada (NSA, 2014).

[27] Unidad de información igual a un septillón.

IMAGEN 2
RECOLECCIÓN DE DATOS DEL CENTRO DE UTAH



Fuente y Elaboración: (NSA, 2014)

El *Utha Data Center* contará con la supercomputadora, que soporta sistemas computacionales de alto rendimiento. El nombre código de la operación es *Cascade* y fue desarrollado con la ayuda de la Agencia de Proyectos de Investigación Avanzada de Defensa (DARPA)[28], asimismo se planea para 2018 desarrollar la primera máquina *exaplop,* es decir que reciba 1 quintillón de instrucciones por segundo (NSA, 2014).

En conclusión, el segundo capítulo de esta investigación cumple el objetivo de determinar las repercusiones en la política de ciberdefensa de Estados Unidos como respuesta a las filtraciones de información clasificada por parte de Edward Snowden. Este capítulo analiza principalmente el caso de Snowden y las revelaciones de los programas de vigilancia y recopilación de datos que la NSA realiza para detener el terrorismo. La controversial filtración lleva a la reformulación de las leyes que rigen el ciberespacio y la agencia responsable de la seguridad nacional, en cuanto a tecnología. Se crea un preámbulo, que introduce el cambio de mandato de Bush a Obama, en especial sus maneras distintas de gobernar. Obama, en sus discursos promete mejorar la infraestructura cibernética del país y reconoce al quinto dominio como un activo importante en el desarrollo nacional. Al poco tiempo de su mandato, WikiLeaks decide filtrar información

[28] Agencia de Proyectos de Investigación Avanzada de Defensa o Defense Advanced Research Projects Agency: agencia estadounidense parte del Departamento de Defensa que es responsable del desarrollo tecnológico de uso militar.

clasificada de las operaciones militares y cables diplomáticos de Estados Unidos, lo cual enfatiza la necesidad de fortalecer el ciberespacio. Dos años después de la revisión y aplicación de una nueva ciberestrategia, Edward Snowden filtra documentos de la NSA. El ex contratista de la agencia y de la CIA, revela información clave que demuestra la falsedad del discurso de Obama, dado que exhibe las mismas características que fueron criticadas del gobierno de su antecesor. Las revelaciones generan malestar entre los ciudadanos que ven invadida su privacidad, y la comunidad internacional que critica las acciones de Estados Unidos.

A manera de contrarrestar la opinión pública nacional e internacional, se decide revisar las políticas de vigilancia y realizar cambios sustanciales en cuanto a las atribuciones de la NSA. Se debate el hecho de encontrar a Snowden como un traidor o un héroe de su país; por un lado, informa a los ciudadanos las preocupantes acciones que su país toma en contra de ellos y a su vez, da una muestra de la capacidad real de la inteligencia estadounidense; los criminales y terroristas cambian sus maneras de ocultar su información, lo cual también lleva a la agencia a reformular sus procesos y tácticas de detección de terrorismo. Sin embargo y a pesar de que Snowden logra cuestionar las estrategias estadounidenses, la hegemonía de este país o se ve afectada ya que después de tres años, la imagen de Estados Unidos ha sufrido poco y su poder a nivel internacional se mantiene. El objetivo de Snowden era crear conciencia tanto para los ciudadanos como para el gobierno, puesto que la cantidad de información sobrepasaba su capacidad de análisis. Esto demostró que Estados Unidos debe modernizar y mantener la vanguardia tecnológica, si no desea que otros actores revelen información vital para sus operaciones. A su vez, da una muestra clara del poder de Estados Unidos dentro del sistema internacional y de su gobierno dentro de su territorio.

CAPÍTULO III

HEGEMONÍA DE ESTADOS UNIDOS FRENTE A ACTORES NO ESTATALES EN EL SISTEMA INTERNACIONAL

3.1. El poder de Estados Unidos versus Snowden en el quinto dominio

Los Estados se han constituido como actores principales o únicos en varias teorías de las Relaciones Internacionales; con la globalización, el sistema internacional se modifica y convierte a los Estados en actores dependientes unos de otros, sus decisiones tienen repercusiones globales, además surgen otros actores que ejercen presión y tienen otros intereses (Acevedo, 2013). Sin embargo, no todos poseen las mismas capacidades y recursos para injerir y moldear el mundo basado en sus intereses (Arenal, 2009).

Según Keohane (1984), Estados Unidos después de la Guerra Fría, se establece como el hegemón debido a que posee una preponderancia de recursos como la supremacía militar y económica (Parma, s.F.). Por otro lado, como Keohane y Nye (1977) establecen, dada la globalización y la injerencia de instituciones supranacionales, multinacionales y transnacionales ajenas al Estado, la agenda internacional se modifica; por lo tanto, Estados Unidos se torna sensible a las decisiones e intereses de otros actores.

El final de la Guerra Fría cambió el panorama internacional y las estructuras de poder para los Estados-nación tradicionales. La globalización provocó una creciente interdependencia y asimetrías entre los actores, que a su vez dejaron de ser sólo los Estados. Individuos, instituciones y organizaciones no gubernamentales ejercieron poder dentro del sistema internacional. Se analizará el juego de poder de los actores, en sus políticas y acciones, y finalmente las repercusiones de las mismas en la interdependencia compleja bajo el marco del caso de las filtraciones de información clasificada de la Agencia Nacional de Seguridad estadounidense (NSA) por parte de Edward Snowden, ex agente de la CIA y NSA.

Este apartado analiza a los actores principales del caso y las capacidades que han probado poseer. Dentro del marco de la interdependencia compleja y el *smart power*, Estados Unidos, la NSA y Snowden juega un rol importante pues demostrarían que el ciberespacio disminuye las asimetrías y permite a los actores hacer uso de sus recursos de manera más equitativa. Así también se resalta la importancia de la información como fuente de poder.

3.1.1. Capacidades y recursos de Estados Unidos en el ciberespacio

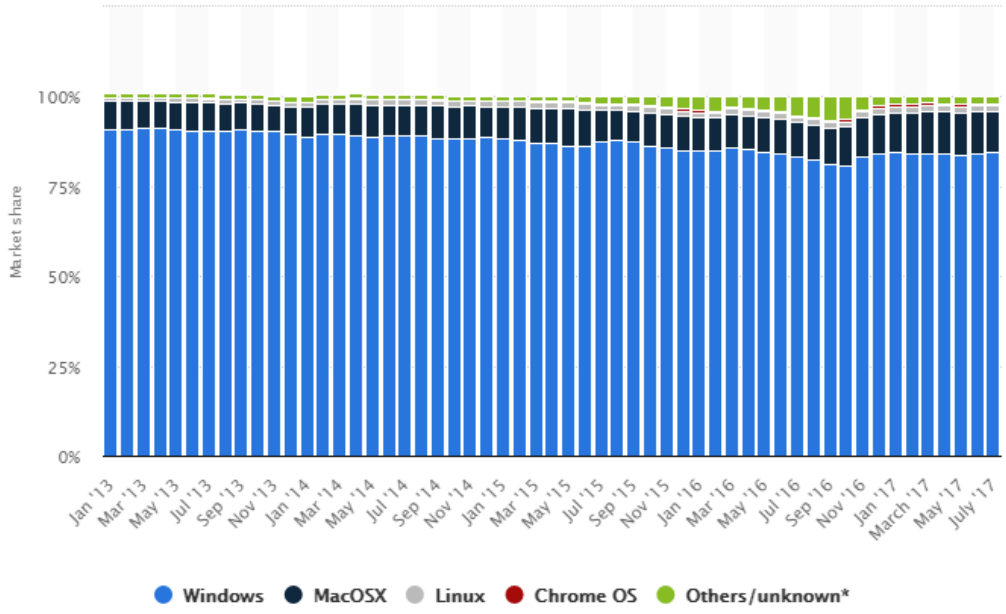
El ciberespacio, al igual que otros dominios, logra determinar las capacidades de un actor. Cabe recalcar que en la interdependencia compleja, la estructura del poder cambia y altera su distribución (Keohane & Nye, 1977). Este hecho que se ve acentuado en el ciberespacio ya que existe un traspaso de poder de Estados a otros actores, por lo tanto el sistema internacional deja de ser un espacio estatocéntrico para convertirse en multicéntrico, pues los Estados por sí solos no consiguen resolver las problemáticas mundiales (Acevedo, 2013). A pesar de todo, los Estados continúan teniendo un rol dominante frente a otros actores, pero al mismo tiempo su vulnerabilidad aumenta debido a la dependencia creada por la tecnología (Nye, 2010).

El Estado, incluso en el ciberespacio, se establece como hegemón dado que influyen en el orden mundial y poseen los recursos tanto económicos, como políticos y físicos. Además, estos están encargados de proveer un ambiente propicio para el desarrollo integral de las operaciones en el ciberespacio. Los gobiernos aplican tanto el *soft power* como el *hard power* para obtener los resultados deseados. El *soft power* es aplicado cuando se realizan alianzas estratégicas y se crean campañas para influenciar la opinión pública (Nye, 2010). Es de esta manera que se creó que Ley de Ciberseguridad del 2015, en la cual se establece la cooperación entre el sector público y privado. Los ataques cibernéticos tanto a los sistemas del gobierno como a empresas e individuos enfatizó la necesidad de una alianza, que permita compartir información. El caso más relevante fue el apoyo de *Sony Entertainment* al gobierno, pues en 2014 se filtró información sobre sus actividades (Peterson, 2014).

El *hard power* se lo observa través de los subsidios al desarrollo de infraestructura, educación y protección de propiedad intelectual. Es de esta manera que Estados Unidos hace uso de la coerción y control legal cuando un individuo u organización no cumple con sus estándares (Nye, 2010). A través de la ley FISA, Estados Unidos obliga a empresas como Google, Apple y Microsoft a proporcionar información sobre sus usuarios, a pesar de ser empresas privadas que no tienen relaciones con el gobierno (Simcox, 2015).

Ejercer poder dentro del ciberespacio depende de siete puntos estratégicos. El primero hace referencia a los sistemas operativos, dado que son estos los que permiten el buen funcionamiento de la mayoría de aparatos electrónicos. Es mercado está notoriamente dominado por Microsoft Windows 86.06%, seguido por Apple 9,18%, Linux 1,24% y Chrome 0,36% (Bejarano, Poder blando frente a poder duro en el ciberespacio, 2013). El gráfico 8 muestra que casi el cien por ciento del mercado es controlado por empresas estadounidenses, que a pesar de pertenecer al sector privado y estar regidas bajo sus propias políticas, su nacionalidad también las condiciona (The Statistics Portal, 2017). Esta situación se da debido a que los Estados están encargados de las políticas que regulan al sector privado, por ejemplo política fiscal y tributaria; los subsidios a desarrollo, investigación o infraestructura, y finalmente, las leyes de protección a los derechos de propiedad intelectual (National Academy of Engineering, 1992). En cuanto a los sistemas operativos de teléfonos celulares, se encuentran dominados por Android de Google, iOS de Apple y Microsoft Windows (The Statistics Portal, 2017).

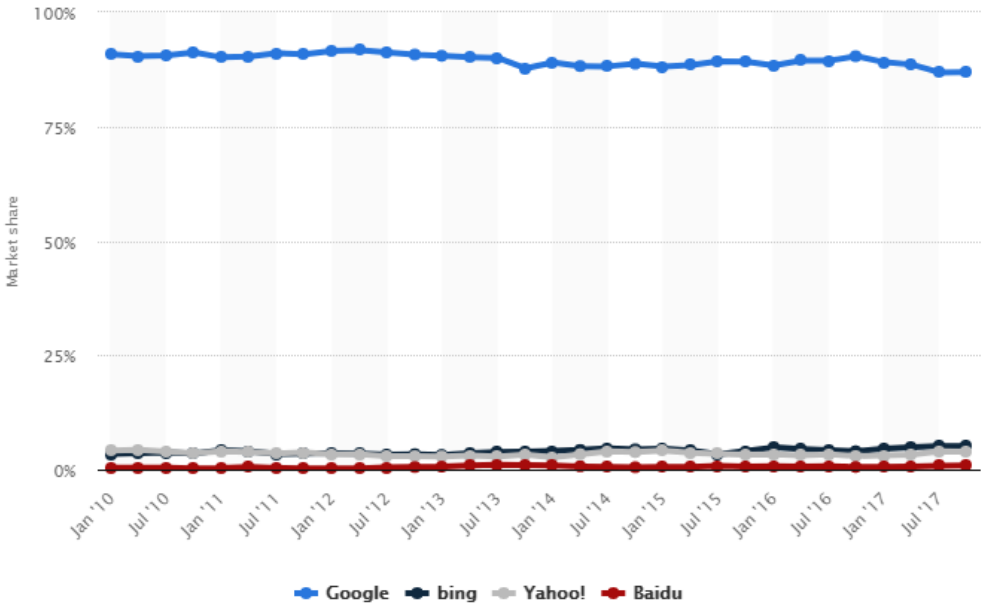
GRÁFICO 8
MERCADO GLOBAL DE SISTEMAS OPERATIVOS 2013 – 2017



Fuente y Elaboración: (The Statistics Portal, 2017)

El segundo punto estratégico son los motores de búsqueda, los cuales tienen la capacidad de mostrar la información más relevante para sus intereses dentro de los resultados de búsqueda. Es decir que las búsquedas en internet están parcializadas por el motor de búsqueda que se utilice (Bejarano, 2013). En este caso, se observa en el gráfico 9 que Google lidera el mercado mundial con 90%, seguido por Bing, Yahoo!, y finalmente Baidu. Los tres primeros que representan el 98%, atribuido a empresas estadounidenses, mientras que el último es una empresa China, la cual lidera en este país.

GRÁFICO 9
MERCADO GLOBAL DE MOTORES DE BÚSQUEDA 2010 – 2017



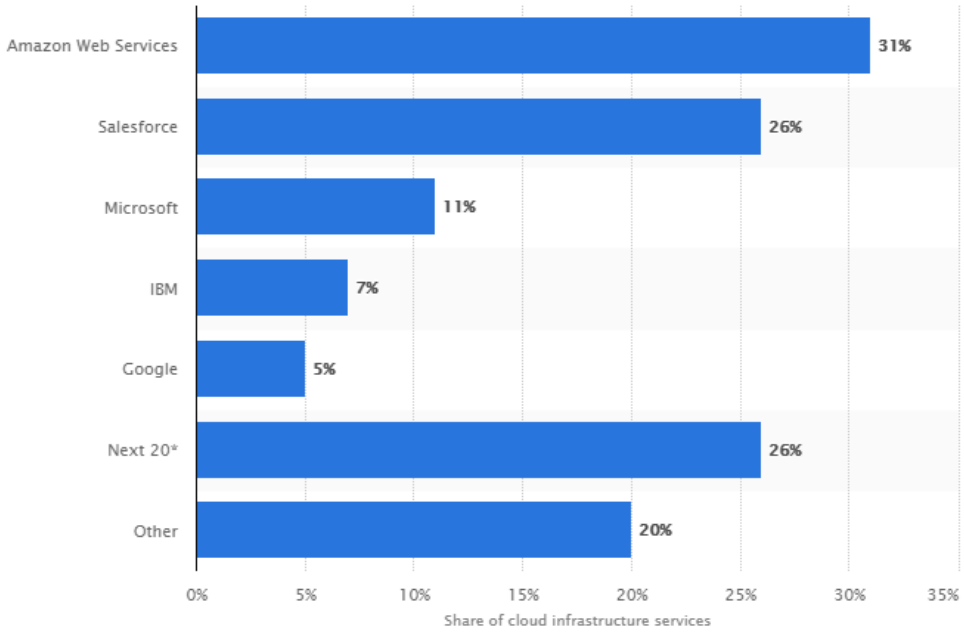
Fuente y Elaboración: (The Statistics Portal, 2017)

El tercer punto estratégico es la infraestructura de telecomunicaciones, los cuales están encargados de proveer el servicio de internet. Debido a los constantes ataques que recibe Estados Unidos de otros países, las centrales de comunicaciones dejaron de ser centralizadas en este país. Otros países han comenzado a invertir en estas tecnologías con el fin de proteger y administrar de manera más precisa sus comunicaciones electrónicas. La innovación y rápido desarrollo de la tecnología ha permitido que los costos de las infraestructuras sean accesibles (Bejarano, 2013).

Nye (2010) aseguró que la información es poder, y el ciberespacio se ha convertido en el guardián de esta. Por lo tanto, la tendencia de almacenar de manera digital se ha acrecentado, lo cual hace referencia al cuarto punto estratégico, el almacenamiento en la nube. En el gráfico 10 se observa que el mercado está dominado al 80% por las empresas de nacionalidad estadounidense Amazon 31%, Salesforce 26%, Microsoft 11%, IBM 7% y Google 5% (The Statistics Portal, 2016). Esta tendencia muestra que los usuarios tienen confianza

en que su información más sensible está resguardada por estos proveedores de servicios y, por ende confían en el país de origen (Bejarano, 2013).

GRÁFICO 10
MERCADO GLOBAL DE PROVEEDORES DE SERVICIOS DE ALMACENAMIENTO DIGITAL 2016



Fuente y Elaboración: (The Statistics Portal, 2016)

Finalmente, los tres últimos puntos estratégicos se refieren a los foros de gobernanzas, criptografía y protocolo. La gobernanza son las alianzas que se forman entre países, empresas, instituciones o individuos, por lo tanto no existe un poder dominante visible, pues está basado en cooperación. La criptografía y protocolo hablan de procesos tecnológicos que permiten el diseño de la arquitectura digital. La criptografía está determinada en Estados Unidos por el Instituto Nacional de Estándares y Tecnología[29], coordinado con la NSA y está impuesto en su territorio como el cuerpo de certificación de esta actividad. El protocolo es el sistema en general de Internet, el cual está liderado por Estados Unidos, quien provee un servicio más completo y seguro, pero desde 2004 China intenta desarrollar su propio protocolo que abarque mayor capcidad y eficiencia (Bejarano, 2013).

[29] NIST: National Institute of Standards and Technology

3.1.2. La agencia Nacional de Seguridad: las estrategias de las instituciones

Las instituciones en la interdependencia compleja adquieren un poder diferente y un rol más representativo en el sistema internacional. Aquellas que pertenecen al Estado se convierten en delegados del mismo y actúan de acuerdo a sus funciones establecidas, lo cual implica que se impongan normas acerca de sus actividades. Estas canalizan la cooperación tanto con actores no estatales como dentro del sector público. Sin embargo, depende del área a la que esté enfocada para hacer mayor uso del *hard power* o *soft power* (Keohane & Nye, 1977). En Estados Unidos, el Departamento de Defensa y la Agencia de Seguridad Nacional tratan de combinar ambos poderes para crear una estrategia de *smart power*. Además la interdependencia ha complejizado las funciones de las agencias estatales, que gracias a la importancia de la difusión de la información necesitan mejorar la transparencia frente al público (Stone, 2008).

La NSA recibe órdenes directas del gobierno con el fin de, mediante procesos cibernéticos, rastrear a posibles criminales y proceder a su detención. Estas tácticas fueron expuestas por Edward Snowden en 2013, lo que reveló que las funciones de la agencia constituyen una violación a los derechos civiles, establecidos en la Cuarta Enmienda que prohíbe las invasiones arbitrarias y protege el derecho a la privacidad (Greenwald, 2014). En este caso, juega un papel importante la transparencia de las instituciones debido a que la credibilidad se obtiene bajo un proceso que se rija por normas y que hasta un punto específico sea público. Incluso para que el *soft* power actúe de manera eficiente, es primordial utilizar la transparencia (Nye, 2004).

La transparencia también constituye una forma de mantener la ciberseguridad, porque elimina la incertidumbre de otros actores acerca de las actividades que realiza la agencia (Popa, 2015). El gobierno de Estados Unidos, en especial en sus leyes de regulación de la NSA, ha dejado varios vacíos legales que causan una múltiple interpretación y un uso errado. El caso más importante radica en la ley FISA, que mediante decreto se la cambia para adaptarla a sus

intereses. Esta fue una de las razones por las que Snowden decidió revelar las tácticas de la NSA (Simcox, 2015).

El problema surge cuando Snowden encuentra los programas de espionaje PRISM y *Upstream* como un mecanismo de monitoreo del terrorismo, pero estos programas iban más allá de la recolección de datos de los posibles terroristas, sino que sus búsquedas se expanden a cualquier persona que podría estar relacionada con el mismo. De la misma manera, la NSA se encarga de buscar información acerca de sus empleados, como Snowden pudo comprobarlo en diversas ocasiones (Greenwald, 2014). De esta forma la NSA ejerce control sobre sus objetivos, sin embargo este poder no es legítimo y constituye una clara violación a la privacidad (Nye & Armitage, 2007).

El espionaje constituye un elemento de poder, puesto que permite a Estados Unidos mantener su influencia en el sistema internacional mediante la información recopilada. Sin embargo, los objetivos del gobierno de Obama se ven claramente desviados hacia intereses políticos y económicos al espiar sistemas de funcionarios de gobiernos extranjeros, tal es el caso del presidente mexicano. Incluso, al finalizar el mandato de Bush en 2008, los programas ilegales de espionaje fueron legalizados por el congreso y las leyes que prohibían estas actividades fueron reformuladas para permitir que la NSA desarrolle dichos programas de vigilancia (Mamritsova, 2018).

En el ciberespacio, la hegemonía se maneja de la misma manera que el mundo físico. Existen reglas, instituciones y regímenes que gobiernan las relaciones entre los actores, y el poder se traduce en los recursos que cada uno posea (Santana, 2017). Los Estados, desde esta perspectiva, continúan administrando el ciberespacio, puesto que son ellos los cuales tienen el deber de crear un ambiente propicio para que el resto de actores interactúe. Es decir que tanto individuos e instituciones aceptan los beneficios del orden hegemónico de los Estados. En este contexto y basado en los puntos estratégicos de dominación

del ciberespacio, Estados Unidos es el país que está legítimamente establecido como poder hegemónico (Santana, 2017).

El gobierno de Estados Unidos, después de las filtraciones, se vio en la necesidad de buscar soluciones en cuanto a la transparencia, debido a que ciudadanos nacionales e internacionales consideraron inaceptable que la mayoría de sus operaciones se den de manera secreta. Se creó un debate acerca de las reformas que deberían hacerse, comenzando por la reestructuración de la NSA (Byman, 2014). A pesar de que Estados Unidos es un Estado que posee poder en aspectos económicos y militares, la dependencia hacia sus socios comerciales y la opinión internacional pueden llegar a modificar su comportamiento. El fenómeno de la interdependencia compleja crea estos resultados porque existen efectos recíprocos, es decir las limitaciones y costos de las relaciones internacionales (Keohane & Nye, 1977). En este caso, el hegemón no controla todo porque el poder es distribuido de manera asimétrica y dependen del contexto en el que se encuentre (Creus, 2013).

Desde su creación en 1952, la NSA se ha encargado de la vigilancia a las comunicaciones. Con el desarrollo del internet, sus búsquedas se ampliaron y se convirtió en una actividad crítica para espiar a otras instituciones en el extranjero, obteniendo información para el beneficio de los Estados Unidos (Tamayo, 2013). Sin embargo, estas agencias de inteligencia crean una dependencia en la tecnología, lo cual según Nye (2010), genera vulnerabilidades, que pueden evidenciarse por diferentes organizaciones e individuos como WikiLeaks y Edward Snowden.

3.1.3. Analizando a Snowden: el ciberpoder de los actores no estatales

El ciberpoder, descrito por Joseph Nye (2010) es la obtención de resultados deseados a través de la utilización de recursos tecnológicos. En el ciberespacio, al igual que en el plano físico convergen dos tipos de poderes: *hard power y soft power*. El quinto dominio permite un bajo costo de inversión, anonimato y facilidad de acceso; por lo tanto, los objetivos de un individuo al

entrar al sistema y red de otro actor van desde la obtención de información hasta un ataque de denegación de servicios. Por otro lado, el ciberespacio permite disminuir las asimetrías creadas por la interdependencia, es decir que un individuo adquiere capacidades, frente a organizaciones y gobiernos, que antes no poseía y suponen una ventaja para el mismo.

Al analizar el caso de Edward Snowden, se puede observar la presencia de dos actores opuestos en sus capacidades físicas, pues en los otros cuatro dominios, el individuo se muestra indefenso frente a un Estado (Arenal, 2009). Ahora bien en el ciberespacio, Snowden es capaz de hacer uso del poder contra Estados Unidos. En este caso, el individuo hace uso de ambos poderes, tanto *hard power* como *soft power* (Nye, 2010).

La estrategia de Snowden está basada en el *smart power*, dado que hace uso de los ataques SCADA[30] al obtener información de manera ilegal, haciendo uso de sus ventajas como consultor. Esta acción está considerada como *hard power*, en contraste con la utilización de esta información para crear una campaña que moldea e influencia la opinión pública e internacional con respecto a las actividades secretas de Estados Unidos, así como una forma de protesta frente a las mismas (Nye, 2010).

En particular sobre la sustracción de información, se puede decir que el poder reside en la difusión de la misma. En la era de la tecnología, la información se traduce en poder y aquel que tenga el control sobre ésta puede llegar a inhabilitar a un actor. Más aún, la información tiene la capacidad de legitimar el poder de un actor porque puede cambiar la percepción y opinión de varias personas (Mamritsova, 2018). Snowden, logró extraer la información de manera que la NSA no tuvo conocimiento hasta que los documentos empezaron a ser publicados. Cabe recalcar que, al ser un experto en tecnologías, Snowden usó las debilidades y ventajas presentes en la dependencia de Estados Unidos en la tecnología (López, 2014).

[30] Supervisión, control y adquisición de datos

Por otro lado, el uso del *soft power* estuvo basado en la creación de una campaña que cambiaría la opinión que los ciudadanos mundiales tienen de Estados Unidos. Después de la sustracción de información, Snowden se dirigió a Hong Kong para reunirse con periodistas, elegidos estratégicamente. *The Washington Post,* periódico estadounidense, *The Guardian* su homónimo en Reino Unido e investigadores internacionales. Con la ayuda de ellos se realizó una selección de las noticias que serían filtrarlas progresivamente, y de la misma manera se pidieron permisos que respaldaban legalmente a los periodistas, en especial en Reino Unido (López, 2014).

A continuación, Snowden salió del anonimato y legitimó la información que estaba proporcionando, al demostrar su relación con el gobierno de Estados Unidos mediante sus consultorías en las agencias de la CIA y NSA. Ambas agencias quedaron en evidencia y conforme con lo expuesto no consiguieron negar los testimonios y documentos presentados en su contra; conjuntamente la NSA hizo públicos en su sitio web los documentos (NSA, s.F.).

"El Ciberpoder" de Joseph Nye (2010) detalla las desventajas para un individuo dentro del ciberespacio, las cuales hacen referencia a las leyes y normas por las que los individuos están regidos. Nye especifica que si se descubre la identidad del criminal, se puede seguir la acción legal correspondiente. El problema reside en identificar al hacker, lo cual se estimó en una entrevista realizada a Mark Lanterman, Jefe de Tecnología de *Computer Forensic Services,* es posible en aproximadamente el uno por ciento de los casos (Brown, 2014).

Snowden está enfrentando una demanda legal por espionaje, razón por la cual no regresa a Estados Unidos. Edward Snowden se encuentra en Moscú como residente, dado que al momento de abordar su vuelo desde Hong Kong a Rusia, de camino a América Latina, su pasaporte fue cancelado por su gobierno. Mientras todavía residía en Hong Kong, Estados Unidos pidió su extradición, que por falta de prueba fue rechazada. El mismo suceso ocurrió en Rusia, pues Vladimir Putin rechazó el pedido. Snowden declaró que la condición para regresar a su país y enfrentar los cargos en su contra es que se realice un juicio justo y público sin

embargo, Snowden piensa que no va a ser factible (Simcox, 2015). Esto se da porque hace 10 años, Thomas Drake, exfuncionario de la NSA, denunció las mismas actividades y fue despedido, a su vez enfrentó varios cargos en su contra, que después de un par de meses fueron desestimados, pero que lo arruinaron financiera y profesionalmente (The Guardian, 2016). El hecho que no puedan llevarse a cabo las acciones legales en su contra, demuestra que las desventajas de las actividades en el ciberespacio poseen un bajo porcentaje de riesgos para los "criminales", incentivándolos a continuar con estas prácticas (Nye, 2010).

La interdependencia compleja determina que el poder se ve afectado por los avances tecnológicos y las comunicaciones. El poder se ve ramificado y pasa a depender del contexto en el que se encuentre. Keohane y Nye (1977) lo clasificaron en términos de sensibilidad y vulnerabilidad para entender el manejo del poder en el sistema internacional, en el cual convergen también actores como individuos que antes no serían tomados en cuenta. Snowden representa claramente dicha situación y llega a pertenecer a la tercera dimensión del Juego de Ajedrez de tres dimensiones, pues es en esta donde el poder depende netamente del contexto y puede irse alternando entre los actores (Nye, 2009).

Al aplicar las dimensiones centrales del poder (sensibilidad y vulnerabilidad) en el caso de Snowden, se llega a la conclusión que el individuo fue sensible, más no vulnerable frente a Estados Unidos. Los argumentos se centran en su capacidad de respuesta frente a los inconvenientes, denegación de pasaporte y pedido de extradición. Snowden eligió estratégicamente los países donde se refugiaba al conocer la coyuntura entre China y Rusia con Estados Unidos. Así mismo, si hubiese podido arribar a su destino, supuestamente Ecuador, estaba seguro que su libertad no se vería afectada, ya que Ecuador dio asilo a Julian Assange cuando este decidió filtrar información (Simcox,2015). Además, durante su estadía en Hong Kong, Snowden estuvo asesorado por varios abogados que lo ayudaron a huir del país.

Cabe recalcar que Snowden es un individuo que se ampara bajo el poder de un Estado, refiriéndose al caso de extradición. Las leyes para extraditar a un individuo, claramente establecen que se debe tener una causa probable admitida por el país remitente de la solicitud; sin embargo, si este encuentra inocente al individuo está en libertad de rechazar la extradición. En Hong Kong, se alegó que no existían las pruebas suficientes para condenar a Snowden, y en Rusia, se justificaron los crímenes cometidos, dado que se expuso una verdad que ponían en alerta a la comunidad internacional acerca de las actividades ilegales que Estados Unidos estaba realizando (Gupta, s/f).

3.2. Análisis de la política exterior de ciberdefensa y la aplicación del *smart power*

El desarrollo de la estrategia del *smart power* y su aplicación a la campaña de Barack Obama estableció el cambio en la política exterior. Bush usó extensivamente el *hard power*, lo cual fue criticado por todo el sistema internacional. Por lo tanto se convirtió en el objetivo principal, restaurar el poder que tenía Estados Unidos, legitimando su poder y liderazgo (Nye, 2009). Obama, continúa con la Guerra contra el Terrorismo, pero desde un enfoque más humano. Existen quienes critican sus verdaderas intenciones e intentan exponer la verdad, es decir Edward Snowden, quien desafiará a Estados Unidos para probar que el autoritarismo tradicional es característico del estilo de gobierno estadounidense independientemente del presidente de turno (Parmar, 2014).

Este apartado analizará la Estrategia para Actuar en el Ciberespacio del 2011 y la Ley del Ciberespacio del 2015, es decir el antes y después de las filtraciones, bajo el marco de la Interdependencia Compleja; la teoría establecerá la eficacia y eficiencia, así como la sensibilidad o vulnerabilidad de Estados Unidos en su política exterior. Finalmente, analizará, según el *smart power*, la aplicación de este concepto en la formulación de leyes y políticas estadounidenses.

3.2.1. El desafío de la Política Exterior estadounidense: "Estrategia para Actuar en el Ciberespacio" 2011

La interdependencia compleja, según Keohane y Nye (1977) generó nuevas amenazas debido a la incorporación de nuevos actores en el sistema internacional, la distribución de poder, el desarrollo tecnológico, la información y la falta de jerarquización de los temas de la agenda. Por ende los problemas y las soluciones se tornaron más complejos, convirtiéndose en una tarea de los Estados, los actores predominantes, la formulación de políticas que incluyeran todas las problemáticas. Uno de los espacios que ganó protagonismo fue el ciberespacio, el cual representaba un desafío mayor para los Estados pues su rápida expansión, naturaleza cambiante y anonimato, lo convierten en un punto difícil de abordar y regular (Nye, 2010).

En el discurso inaugural de su mandato, Barack Obama (2009) estableció la importancia de regular y aprovechar las capacidades del ciberespacio. El desarrollo tecnológico trajo grandes oportunidades para el progreso del país, pero éstas van ligadas a los problemas y responsabilidades que conlleva el ciberespacio. En 2008, el sistema y red militar en Afganistán fue contaminado por un flash-drive que contenía un virus capaz de navegar a través de la infraestructura digital y sustraer información confidencial de tácticas y estratégicas militares. El incidente fue detectado casi dos años más tarde, lo cual probaba que la infraestructura de los sistemas estadounidenses no estaban equipados para hacer frente al rápido desarrollo tecnológico (BBC, 2010).

La globalización provocó un efecto de pérdida de fronteras y límites entre lo externo e interno, afectando la formulación de la política doméstica y exterior. Los nuevos actores imponen sus intereses y cambian la agenda establecida por los Estados, la militarización disminuye porque la seguridad no es el tema predominante; así también la interdependencia se basa en términos de costos y beneficios que surgen de las relaciones entre actores (Acevedo, 2013). WikiLeaks y Snowden constituyen un cambio importante en la forma de hacer política para los Estados Unidos. Instituciones e individuos logran anteponer sus intereses

frente a un Estado para que la política exterior sea reformulada en pos de la comunidad (Tamayo, 2013).

La cooperación es más efectiva para lograr los objetivos e intereses frente a amenazas comunes. Además, la interdependencia complejiza la autonomía de los Estados ya que estos no son capaces de resolver los problemas sin ayuda de otros actores (Keohane & Nye, 1977). Estados Unidos, en 1946 crea una alianza estratégica que se mantiene hasta la actualidad, el tratado UKUSA que permite el intercambio de información entre agencias de inteligencia en cinco países aliados. El interés de espionaje como forma de seguridad después de la Segunda Guerra Mundial y, actualmente como herramienta para actuar en la ciberguerra ha sido el objetivo primordial de la cooperación para estos países (UKUSA Agreement, 2016).

La Estrategia para actuar en el ciberespacio, creada en 2011 como marco regulatorio de las funciones de las agencias y departamentos estatales, presentó cinco estrategias. Estas están basadas en la estrategia del *smart power*, que requiere un balance para el funcionamiento correcto de las operaciones en el ciberespacio. La estrategia 1 se basa en aprovechar el potencial que ofrece el ciberespacio a través de una mayor capacitación, crear redes seguras y una coordinación conjunta entre departamentos y agencias (Department of Defense, 2011). La estrategia está orientada al *soft power* mediante la educación, la mejora de sus sistemas y la cooperación (Nye, 2009).

La segunda estrategia se enfoca en nuevos conceptos para la adaptación al ciberespacio, lo cual sigue en el lado del *soft power*, pero la estrategia falla cuando Estados Unidos no presenta la capacidad de respuesta frente a las filtraciones porque no pueden descifrar la cantidad real de documentos que Snowden sustrajo (Department of Defense, 2011). Edward Snowden en una entrevista declaró que dejó pistas rastreables para que Estados Unidos comprenda e identifique los documentos que filtró para que se pueda crear un plan de acción basado en una

información específica, lo cual según sus mismas declaraciones, Estados Unidos es incapaz de hacer (Kirk, 2014).

El uso del *soft power* es evidente en la estrategia 3 y 4, enfocados en las alianzas internas y externas. La cooperación constituye un entendimiento de la interdependencia y la importancia de la unión de capacidades y recursos para la mitigación de amenazas y logro de objetivos. De manera interna, las alianzas interestatales permiten la recolección de información y coordinación de esfuerzos, pero la insuficiencia de recursos provoca que la información se desborde del análisis y a su vez que las interpretaciones de la misma sean contradictorias. Esto repercute en la toma de decisiones de las medidas correctivas oportunas. Por otro lado, la cuarta estrategia dirigida a las alianzas interestatales se rige bajo el marco de la cooperación, cuando Obama (2009) declara que el ciberterrorismo es una amenaza mundial que debe ser vencida de manera conjunta. Los tratados con Reino Unido y el grupo *Five Eyes* proporcionan información y planes de acción que al igual que en la estrategia 3, resultan en un exceso de información que no puede ser analizada a tiempo para actuar (Department of Defense, 2011).

Finalmente, la estrategia 5 del desarrollo e innovación tecnológica busca una mejora de la rapidez de acción frente a amenazas, que puede ser tomada como una medida a largo plazo, puesto que se establece como un proceso de prueba y error. Esta estrategia se basa en el *soft power* y *hard power*, dado que la aplicación de esta tecnología se traduce en sistemas de ofensa y defensa (Department of Defense, 2011).

Keohane y Nye (1977) determinaron que el poder está identificado en dos dimensiones: la sensibilidad y vulnerabilidad. Snowden, gracias a su posición dentro de la NSA logra sustraer información confidencial y vulnera los sistemas de la agencia, pero la mayor falla presente en este caso es la falta de respuesta al incidente, dado que Estados Unidos no detecta esta invasión hasta que se publican los documentos. El resultado es la reestructuración de las funciones de la agencia y una inversión de mil quinientos millones de dólares para mejorar y expandir los procesos de almacenamiento de información (NSA, 2014). Su incapacidad de

adaptarse a los cambios constantes del ciberespacio provoca la reformulación de políticas y el cambio constante de leyes. También cede sus intereses por las acciones de un individuo, demostrando que el poder de Estados Unidos fue vulnerable en el ciberespacio frente a instituciones e individuos por su dependencia en los procesos digitales y la disminución de las asimetrías (Nye, 2010).

3.2.2. Ley del Ciberespacio 2015 y marco jurídico como fuente de poder

Los Estados hacen uso de sus capacidades y recursos para ejercer poder en los otros actores, puesto que son los Estados los que se benefician de la aplicación de las leyes, como la de Espionaje, Patriot Act, entre otras (Mamritsova, 2018). El caso del uso de la Ley de Espionaje en Estados Unidos, que protege la información nacional se usó en contra de Snowden, cuando el individuo hizo uso de sus capacidades para publicar la información confidencial (Yoon, 2015). La utilización del *hard power* se ve de manera clara, pero también se denota su incapacidad de llevarlo frente a la justicia para que sea condenado por los crímenes que se le imputan. Al momento, Edward Snowden reside en Moscú, Rusia gracias al asilo concedido por este país, a pesar que más adelante Estados Unidos solicitara la extradición de Snowden, ésta fue denegada (Simcox, 2015).

Por otro lado, Estados Unidos infringe la Ley de Espionaje y la Cuarta Enmienda de su constitución al monitorear las comunicaciones de sus ciudadanos. No obstante, las repercusiones legales para el gobierno no han sido significativas, dado que, debido a la reformulación de la ley mediante la restricción el almacenamiento de metadatos, las acciones de la NSA han quedado en la impunidad (Simcox, 2015).

El *Patriot Act* es la ley que permite a Estados Unidos recopilar metadata en caso de un posible ataque terrorista y siempre que exista una causa probable (Simcox, 2015). El gobierno de Obama espía a sus empleados y contratistas para prevenir la traición; sin embargo, Snowden creó una ventaja de la misma estrategia y doblegó los esfuerzos de este país, exponiéndolo frente al mundo

(Simcox, 2015). Se evidencia de esta manera que en el ciberespacio, las capacidades de los individuos son mayores que en el mundo físico, sin embargo para adquirir poder y afectar la hegemonía de un país es necesaria la legitimación por parte de la comunidad internacional (Keohane, 1984).

La Ley de Vigilancia en el Extranjero es la estrategia más usada del *hard power* por Estados Unidos. A través de esta se recopilan datos de ciudadanos de todo el mundo cuando existe una sospecha de terrorismo. Así mismo esta permite investigar al entorno del criminal a escala internacional (Simcox, 2015). Se usa esta ley y se la modifica para adaptarla a sus intereses. Por lo tanto, la coerción legal se usa por los Estados para cumplir sus objetivos y, al ser actores dominantes, las repercusiones de sus actos no son tan significativas, ya que sus acciones se encuentran amparadas bajo una ley, la cual es fiscalizada por sus instituciones. A través de las leyes, los Estados tienen un rango mayor de acción.

Las revelaciones de Snowden modificaron las políticas de la NSA y el gobierno, así como sus procesos. Se logró que mejoren la transparencia, que se restrinja la información que se provee a los empleados y se mejoren las tácticas de detección de amenazas. Se establecieron dos leyes importantes: *Freedom Act* y la Ley de Ciberseguridad. Sin embargo, el objetivo general de Snowden fue logrado parcialmente, pues Estados Unidos continua con la recopilación de datos y espionaje mundial, así también como una respuesta vaga del sistema internacional que falló en condenar las acciones de Estados Unidos (Simcox, 2015). Esto se da debido a que como Keohane (1984) establece, la hegemonía no está en declive, sino que se transforma gracias a la interdependencia. En este caso, la cooperación adquiere un rol importante que permite que otros actores se involucren, pero siempre existe un hegemón que mantiene un poder asimétrico.

El *Freedom Act* actuaría como una ley regulatoria y de control del espionaje, en especial aquel de los metadatos. De la misma manera, impide la formulación de leyes secretas y fomenta la introducción de un defensor público dentro del FISC, el cual también necesitará de mayor documentación para permitir el espionaje; finalmente, la ley obliga al Estado a desclasificar los fallos del juez

en casos de terrorismo (Reitman, 2015). Un efecto de la ley, también es la iniciativa del sector privado que impone sus intereses mediante una coalición para reformar la vigilancia y mejorar la encriptación de sus sistemas (Amnistía Internacional, 2015).

En 2015, se firma la Ley de Ciberseguridad para crear un intercambio voluntario de información con el sector privado acerca de tácticas y detección de amenazas. Se promueve en el mismo la transparencia, la privacidad y el respeto de la información clasificada de cada entidad. Lo cual constituye una herramienta del *soft power*, la cooperación (Department of Homeland Security, 2015).

En cuanto a las leyes internacionales que rigen para este caso, encontramos a la Convención de Budapest y UIT. En el sistema internacional, después de la hegemonía tradicional, la cooperación se convirtió en el sistema imperante, la cual es la encargada de procurar la estabilidad que el Estado hegemón daba; no obstante, la cooperación necesita de un país o grupo de países que lidere los procesos (Keohane, 1984). Bajo este contexto y después de las revelaciones de Snowden, la UIT declaró su posición de alentar a la comunidad internacional a crear tratados que prevengan el cibercrimen, en especial el espionaje.

De la misma manera, bajo el marco de la Convención de Budapest, la cual Estados Unidos firmó y ratificó, los crímenes que se cometen en el ciberespacio deben ser penados bajo las leyes de cada país. Sin embargo, la gran deficiencia de este tratado radica en la adopción de la misma, puesto que solo 44 países (hasta el 2016) la han ratificado, lo cual permite que en países donde no se ha aceptado, los criminales tienen mayor capacidad de acción (Council of Europe, 2014). Cabe recalcar que ni China, ni Rusia han firmado, ni ratificado la convención. Además, Budapest da parámetros que los países han tratado de seguir, pero el avance tecnológico aumenta cada día y sin precedentes, complicando el desarrollo de una política que cubra las necesidades del momento. En cuanto a las leyes internacionales, a pesar de que sus objetivos están dirigidos a la penalización del crimen en internet, no ha existido una acción en contra de Estados Unidos o

Snowden por las revelaciones, lo cual implica que todavía no hay un consenso claro dentro del sistema internacional (Miles, 2013).

En cuanto a la cooperación bilateral o multilateral de Estados Unidos con países como Gran Bretaña, Australia, Nueva Zelanda, entre otras naciones, se puede observar que estos países pueden convertirse en la nueva hegemonía compuesta como una red de poder (UKUSA Agreement, 2016). Estados Unidos, en temas cibernéticos está aliado con países poderosos política, económica o militarmente. Esta red busca posicionar una política de poder en el sistema internacional a través de sus programas de vigilancia. Las ventajas que poseen son la preponderancia de recursos que manejan entre ellos (Keohane, 1984).

3.2.3. El *smart power*: ¿existe un balance de *soft* y *hard power* en la política exterior y las acciones de Estados Unidos?

El *smart powe*r es la estrategia que equilibra el *soft power* el *hard power*. Nye (2009) estableció que la utilización de uno solo en la elaboración de la política exterior no produce los resultados deseados por el actor. Esta estrategia basa su accionar en la inteligencia contextual, lo cual significa que el actor conoce el espacio y contexto que está normando y sabe el momento de usar cada poder. La política exterior estadounidense, en discurso, utiliza varios elementos del *soft power* en especial dentro del ciberespacio. Sin embargo, Snowden comprobó que la militarización del ciberespacio es un eje prioritario en la estrategia estadounidense (Tamayo, 2013).

La inteligencia contextual crea una metáfora donde los poderes son distribuidos en diferentes planos, como un juego de ajedrez tridimensional. Las primeras dimensiones hacen referencia al poder militar y económico, en las cuales Estados Unidos el actor predominante. Sin embargo, en la tercera dimensión, donde se encuentra el ciberespacio, el poder se distribuye en diferentes actores, según la problemática. Por lo tanto, en este plano, actores no estatales como individuos logran ostentar el poder de acuerdo al contexto(Nye, 2009).

En el ciberespacio, Estados Unidos y Snowden poseen capacidades similares y los gobiernos aumentan su vulnerabilidad, sin embargo, un individuo no puede llegar a tener los recursos necesarios para desestabilizar a un hegemón (Keohane, 1984). Por lo tanto, aunque el *smart power* es una iniciativa que nace en Estados Unidos, con el gobierno de Obama (Nye, 2009), la confianza que tiene este país en el *hard power* para la resolución de problemas a corto y mediano plazo, hizo que se militarice el ciberespacio (Tamayo, 2013).

En 2009, se creó el USCYBERCOM que trabaja bajo las órdenes del Comando Estratégico de los Estados Unidos para desarrollar operaciones ofensivas y defensivas. Su objetivo es alcanzar la superioridad estratégica, para lo cual es necesario estar preparado y ser el primero en atacar, la lógica detrás de esta afirmación se basa en que al tener las capacidades ofensivas existen más posibilidades de ganar y mantener la iniciativa (Tamayo, 2013).

Nye (2012) asegura que el ciberespacio se encuentra en medio de una guerra, donde la información constituye la principal arma, por lo que el espionaje es un componente esencial al momento de adquirirla. Mediante el espionaje se recolecta conocimiento e inteligencia, pero de ser detectado crea tensiones y provoca la ruptura de las relaciones. Los actores participan en una ciberguerra porque a diferencia de la guerra convencional, en el ciberespacio, el espionaje es fácil y no requiere de grandes inversiones del presupuesto, así también es veloz, consigue mayor información con alcance global y mantiene el anonimato. Por lo tanto, es un espacio que se encuentra en disputa para moldearlo bajo los intereses del actor que logre obtener el poder, como en el resto de dominios (Tamayo, 2013).

3.3. La legitimación de la hegemonía estadounidense

Los Estados se han constituido como actores principales o únicos en el sistema internacional según las teorías de las Relaciones Internacionales, sin embargo, la globalización modifica el sistema y convierte a los Estados en actores dependientes unos de otros, dado que sus decisiones y acciones tienen repercusiones globales; de la misma manera surgen otros actores que ejercen

presión para que sus intereses sean incluidos dentro de las políticas (Acevedo, 2013). Si bien tienen más protagonismo, sus capacidades y recursos para injerir y moldear la política, no son suficientes. Dentro del ciberespacio estas asimetrías disminuyen y los actores no estatales ganan nuevas ventajas frente a los Estados (Nossel, 2004).

A continuación, se analizará si la incidencia de nuevos actores en el ciberespacio permite legitimar el poder de Estados Unidos en el sistema internacional. Primero, se determinará el concepto de ciberguerra en el contexto del caso Snowden, para continuar con el análisis de la hegemonía estadounidense bajo el marco de la interdependencia y el ciberespacio; y finalmente, se establecerá si los nuevos actores eclipsan el accionar de los Estados.

3.3.1. Ciberguerra: la legitimación del uso del *hard power*

El año 2013 se destacó por la revelación más grande e importante de los Estados Unidos. Edward Snowden filtró información confidencial de las actividades de la Agencia Nacional de Seguridad de Estados Unidos (NSA) (THIBER, 2013). En el ciberespacio o quinto dominio, el poder reside en aquel que tiene mayor capacidad de difusión. El anonimato y las reducidas barreras de entrada proporcionados por el ciberespacio, permiten a los actores realizar prácticas desde cualquier punto del mundo, afectando sistemas de gobierno, empresas multinacionales y cualquier individuo conectado a una red (Nye, 2010). La seguridad en el ciberespacio se convierte en una herramienta crucial, pero las múltiples interconexiones, encriptaciones y discreción del mismo, lo convierten en una tarea casi imposible (Clemente, 2013).

Nye (2010) establece que el poder depende del contexto, por lo tanto las asimetrías en el ciberespacio disminuyen incluso para los actores más pequeños, quienes logran hacer uso de sus capacidades mediante los limitados recursos que poseen. Es de esta manera que los actores actúan igual que en otros dominios, tratando de obtener más poder a través de la ciberguerra; la cual puede ser

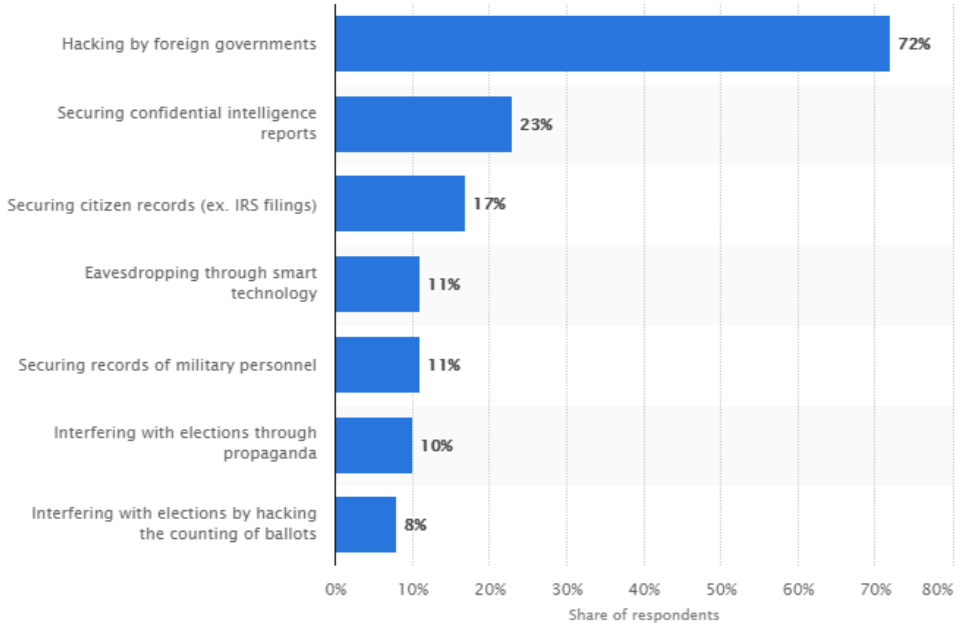
conceptualizada como un conflicto presente dentro del ciberespacio y que utiliza armas no físicas, coerción y persuasión para lograr sus objetivos (Nye, 2011).

En el ciberespacio, por ende no se puede hablar de un actor dominante, de hecho la dependencia que ejerce, provoca nuevas vulnerabilidades para los actores predominantes en otros espacios, y que son aprovechadas por actores no estatales, lo cual produce mayor inseguridad. El fenómeno de los ciberataques no es reciente, pero debido al desarrollo de la tecnología, estos se han diversificado, desde denegación de servicios, espionaje, irrupción hasta destrucción de sitios web. En el espacio físico, la guerra no es rentable de manera económica, aparte sus repercusiones son visiblemente desastrosas por las pérdidas tanto materiales como de vidas inocentes. Sin embargo, la ciberguerra es una guerra donde no se demarra sangre y puede pasar desapercibida, lo cual incita a los actores a introducirse en ella (Nye, 2012).

Estados Unidos, en su ciberestrategia ofensivo-defensiva ha invertido millones de dólares. En 2015, la Ley Federal de Administración de la Seguridad de la Información[31] invirtió 13,1 mil millones en la defensa de los sistemas tecnológicos (The Statistics Portal, 2017). El gráfico 11 muestra que los hackeos[32] de otros Estados a las redes estadounidenses representan el 72% de los ataques cibernéticos. El 23% representa un problema de aseguración de información confidencial, y el 17% va dirigido a la información de los ciudadanos (The Statistics Portal, 2017).

[31] Federal Information Security Management Act (FISMA): legislación estadounidense para la protección de la información, operaciones de inteligencia y activos del gobierno frente a amenazas internas y externas (The Statistics Portal, 2017).
[32] Ataques cibernéticos con el objetivo de recolectar información en un sistema ajeno.

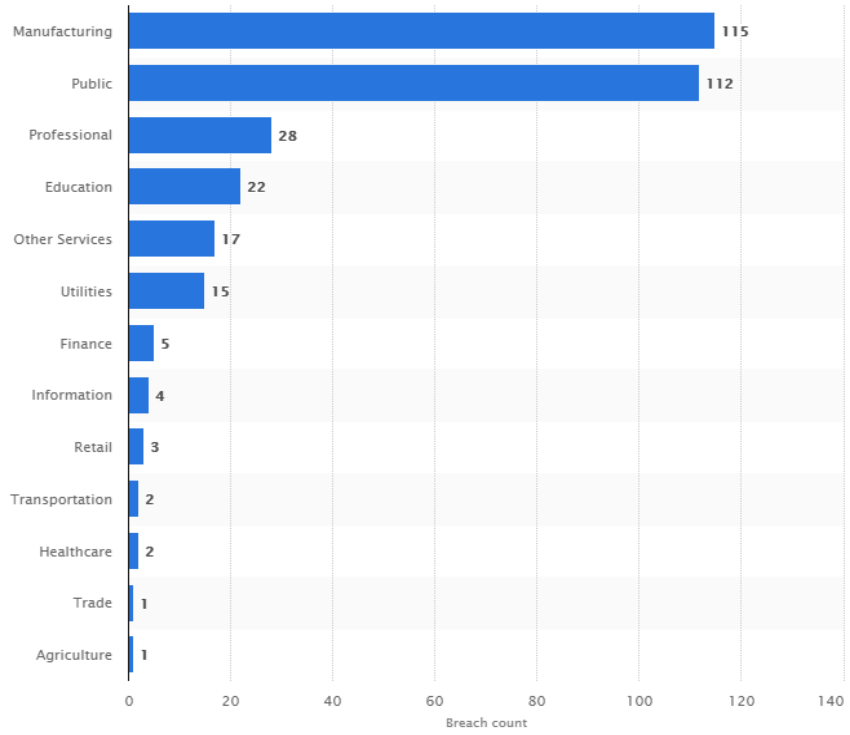
GRÁFICO 11
MAYORES PROBLEMAS DE SEGURIDAD CIBERNÉTICA EN ESTADOS UNIDOS HASTA 2016



Fuente: (The Statistics Portal, 2017)

Cabe recalcar que en el ciberespacio la guerra se da entre actores de diferentes índoles. Los Estados pueden enfrentarse a otros Estados, así como a instituciones, organizaciones e incluso individuos. Sin embargo, las industrias que más ataques de espionaje reciben al año, según una encuesta realizada en 2016 y que se muestra en el gráfico 12, son la industria de manufactura con 115 incidentes llevados a cabo satisfactoriamente al año, seguido por 112 incidentes al sector público.

GRÁFICO 12
INDUSTRIAS MÁS ATACADAS POR EL CIBERESPIONAJE 2016



Fuente: (The Statistics Portal, 2017)

3.3.2. La hegemonía de Estados Unidos post-Snowden

La teoría de la interdependencia compleja (2009), establece que el poder es la habilidad de afectar el comportamiento de otros para obtener lo que se desea. Al utilizar la estrategia adecuada, el poder se legitima y puede llegar a mantenerse incluso en los momentos más difíciles. Estados Unidos, se ha constituido como el hegemón mundial, pues domina la economía mundial y la industria militar en más del 50% (World Economic Forum, 2017). En gran parte, el poder de Estados Unidos radica en el *hard power*, sin embargo la coerción y las amenazas como forma de ejercer poder no duran eternamente. El *soft power* ha probado ser un método más duradero y efectivo de ejercer poder (Keohane & Nye, 1977).

Estados Unidos evoca un sueño, que muchos desean vivir. Este país resalta por su cultura, sus políticas e ideales, dado que trabaja por el progreso de una manera que ningún otro país puede superar, y lo hace a través de un nacionalismo acentuado en cada acción que realiza. Los ejemplos más claros son la industria del

cine, la música y comercial que se encuentran presentes en la vida de la mayoría de ciudadanos en el mundo. Las personas admiran abierta o secretamente sus ideales de libertad; así que a pesar de las fuertes críticas que Estados Unidos recibe por sus políticas altamente militarizadas, sus intromisiones en la privacidad y su excesivo consumismo, probablemente nadie puede decir que no ha visto una película de Hollywood, o tiene ropa de marcas estadounidenses, o incluso ha comido en cadenas de comida rápida como McDonald's o KFC (Nye, 2004).

De la manera en la que Estados Unidos ha ganado su reconocimiento, sus mayores enemigos son aquellos que intentan exponer la verdad de su éxito, y sus recursos son poderosos. La Era de la Información, se convierte en un peligroso adversario debido a la libre información y fácil acceso que internet proporciona (Nye, 2009). Edward Snowden, utiliza igual el *soft power* para transmitir los documentos confidenciales de la NSA, que en un principio afectan a la imagen de Estados Unidos, pero tres años después (2016) el mundo parece haber olvidado que el espionaje es una violación a los derechos civiles. En una encuesta realizada en 2016 acerca de la aprobación a los programas de vigilancia, el 40% de los ciudadanos estadounidenses encuestados aprobó los monitoreos, así también el 54% de ciudadanos de otros países dice estar de acuerdo. En cuanto a los líderes mundiales, el 60% ratificó las acciones tomadas en contra del terrorismo (Rainie, 2016).

No obstante, una de las razones por las que el sistema internacional no ha reaccionado en contra de Estados Unidos es que muchos de los países más influyentes eran sus aliados. Bajo el marco del Tratado *UKUSA*, firmado en 1946 en secreto, el grupo *Five Eyes* ha compartido información acerca de las operaciones de intercepción y decodificación de las comunicaciones interferidas en el extranjero (UKUSA Agreement, 2016). Otra de las razones relevantes tienen que ver con la Interdependencia Compleja ya que la falta de jerarquización de los temas ha provocado un fenómeno, en el cual varios temas surgen al mismo tiempo, por lo que la población se encuentra dividida en diferentes problemáticas (Keohane & Nye, 1977). Temas como la igualdad de género, la inmigración, los

derechos de los grupos LGBTI, las guerras de Medio Oriente y los atentados terroristas han ocupado los recursos y sobre todo la atención de la población mundial (Rieff, 2013).

El problema de la falta de atención a un tema tan controversial es la creciente dependencia que todos tienen en cuanto al ciberespacio. A pesar de saber que los espían continuamente y que las comunicaciones están interceptadas, nadie puede desarrollar sus actividades diarias sin internet, desde una búsqueda de información hasta transacciones de banco. Por lo tanto, y como se estableció previamente, el Estado juega un rol importante dentro del ciberespacio y es aquel de organizar todo su escenario (Bejarano, 2013). Incluso, muchas personas renuncian a su privacidad consciente y voluntariamente al acceder a redes sociales donde exponen cada paso que van a dar en su vida y cuentan su historia completa mediante fotos, publicaciones y videos. Es así que, a pesar de ser inconstitucional, los gobiernos violan la intimidad de los usuarios de Internet mediante las herramientas más fáciles (Rieff, 2013).

Tomando en cuenta la teoría de post-hegemonía de Keohane (1984), Estados Unidos se posiciona como un hegemón tanto dentro del ciberespacio, como en el sistema internacional. Su preponderancia se basa en las alianzas estratégicas con otros países poderosos creando redes de poder. Además, la falta de leyes claras que sancionen los crímenes virtuales de la misma manera que los del escenario mundial, la ventaja que adquiere a través del espionaje y su política de poder que se ha posicionado en el sistema a través del *soft power*, han creado una ideología hegemónica que está presente en la vida cotidiana y hacen relevante a Estados Unidos en la toma de decisiones en instancias mundiales.

3.3.3. Las razones de Snowden: ¿los actores no estatales representan una amenaza?

Las repercusiones de las revelaciones en la imagen y poder de Estados Unidos frente al mundo no fueron lo esperado por Snowden, pues la respuesta internacional no desencadenó mayores reformas (NPR, 2013). Un reporte de

Vodafone[33] habló sobre la necesidad de la transparencia y cómo los países usan la información de las telecomunicaciones en sus programas de inteligencia, lo cual no se había visto antes de Snowden. Empresas como Microsoft argumentaron que Estados Unidos tiene que poner un límite entre privacidad y seguridad nacional para reestablecer la confianza de los usuarios que utilizan en su vida cotidiana aparatos tecnológicos[34]. De la misma manera, los individuos han creado grupos que ayudaran a tomar medidas para fortalecer la privacidad, grupos como Thirteen Principles y Don't Spy on Us (The Privacy Surgeon, 2014).

Keohane y Nye (1977) aumentan la importancia de los individuos y cómo estos logran alterar la agenda, una de las razones de que no exista una jerarquía en los temas. Los individuos poseen capacidades de actuar ofensivamente y generar una amenaza real que resta poder al Estado. De esta manera, observamos que Snowden posee mayores capacidades de eludir la seguridad de Estados Unidos, pero sería un poder limitado o relativo pues las políticas no cambian sustancialmente y el Estado mantiene su poder frente al mundo. En 2015 el Tribunal de Facultades de Investigación falló que la recopilación masiva de información privada de los registros de telecomunicación era ilegal, hecho que cambió las leyes en Estados Unidos (U.S. House of Representatives, 2016).

La información es, actualmente, la mayor fuente de poder que posee un actor. Edward Snowden dijo que debido a su trabajo dentro de las agencias nacionales estadounidenses, obtuvo más información que cualquier otro empleado promedio. En esta situación se hace presente la moral y ética de cada persona, debido que frente a estas actividades ilegales, lo correcto sería denunciarlo. Snowden, en una entrevista con *The Guardian,* dijo que las acciones de Estados Unidos deberían ser determinadas por el público en general, pues son ellos los principales afectados. Así también dijo que no desea vivir en un mundo donde cada conversación o acción que realice, sea grabada y posiblemente utilizada en su contra en algún momento (Snowden, 2013).

[33] Compañía internacional de telecomunicaciones británica (Vodafone, s.F.)
[34] "These concerns have real implications for cloud adoption. After all, people won't use technology they don't trust." Microsoft's General Counsel Brad Smith, 2014

Las asimetrías de la interdependencia compleja, en el ciberespacio dejan de ser importantes, porque este dominio proporciona capacidades y ventajas que los actores no tienen dentro del sistema internacional en otros contextos. Un individuo es incapaz de enfrentarse a un Estado, porque no posee los recursos necesarios, pero el anonimato del ciberespacio equilibra las asimetrías (Nye, 2010). Edward Snowden con sus limitaciones frente a Estados Unidos, fue capaz de revelar información confidencial de este país, sin que él mismo se diera cuenta hasta que los documentos fueron publicados (Simcox, 2015).

Las razones de Snowden, según sus declaraciones, siempre persiguieron el bienestar de Estados Unidos, dado que las capacidades reales de una nación como ésta son superiores a las que sus empleados ofrecen y su infraestructura permite. Este es el país que, técnicamente inventó el internet y es interesante observar que con el paso de los años, la tecnología creció incesantemente pero las capacidades del país no le siguieron el paso (Kirk, 2014).

En conclusión, el tercer capítulo de esta investigación cumple el objetivo de aplicar el *smart power* en el marco de la interdependencia compleja en el caso de Estados Unidos como actor estatal frente a Edward Snowden para determinar la afectación del poder legitimado del país. Debido a las filtraciones ha habido especulaciones de la real afectación al poder general de Estados Unidos, es decir su influencia en los cinco dominios. En el ciberespacio, este país pierde sus ventajas y se vuelve vulnerable, lo cual fue aprovechado por Edward Snowden, quien pudo vulnerar sus sistemas, pero no su hegemonía.

En cuanto a la política exterior en ciberdefensa, muchas de las estrategias fallan por la falta de procesos claros y una falta de coordinación del trabajo en conjunto entre las agencias. Estas estrategias estaban enfocadas en mejorar los sistemas que dos años después fueron vulnerados por Snowden. Finalmente, cuando se analiza la influencia de Estados Unidos, después de tres años de filtrada la información, se infiere que el poder legítimo y la hegemonía del Estado se ven

afectados momentáneamente. Los objetivos de Snowden se cumplen parcialmente porque logra que Estados Unidos cambie sus políticas, invierta en la mejora de sus infraestructuras digitales e incremente la transparencia. En cuanto al objetivo de crear conciencia en el sistema global, acerca de los programas represivos que violan los derechos fundamentales de los seres humanos, no logra alcanzarlo, porque tres años después muchas personas han olvidado estos sucesos y han continuado con sus vidas sin tomar las medidas para evitar estas situaciones.

VII. CONCLUSIONES

El presente Trabajo de Disertación se planteó la siguiente pregunta de investigación: ¿Se ha visto afectada la hegemonía de Estados Unidos por las fallas de seguridad de la Agencia Nacional de Seguridad expuesta al mundo cuando Edward Snowden filtró información clasificada con respecto a las decisiones tomadas en política exterior durante el mandato de Obama? Se escogió proponer esta interrogante, en vez de una hipótesis dado que el tema propone contenidos no explorados a profundidad, y por lo cual permite expandir los conocimientos previos.

Ante este cuestionamiento se puede concluir que la hegemonía de Estados Unidos en el sistema internacional no se vio afectada y su influencia todavía prevalece en la toma de decisiones; sin embargo, dentro del ciberespacio, el poder se distribuye entre los nuevos actores, y los Estados pierden la capacidad de ejercer la misma presión con relación a la política y accionar como lo hacen fuera del mundo virtual. Este fenómeno se da debido al desarrollo tecnológico e interdependencia existentes, que han creado un espacio propicio para que los actores no estatales tengan los recursos y capacidades para influir e interponer sus intereses en la formulación de políticas. Por lo tanto, Estados Unidos es vulnerable dentro del ciberespacio porque la naturaleza cambiante del mismo permite el libre acceso, anonimato y barreras casi inexistentes para todos los actores; no obstante, Estados Unidos goza de un poder hegemónico adquirido con el discurso de la estrategia del *smart power* y el uso del *soft power* mediante la cultura popular, ha convertido a Estados Unidos en el eje del mundo occidental.

A continuación se expondrán las conclusiones que apoyan la respuesta a la Pregunta de Investigación:

- La Interdependencia Compleja es una teoría de las Relaciones Internacionales que se adapta al nuevo modelo que surge después del fin de la Guerra Fría y debido a la globalización. Fenómenos como la

disminución de la militarización, nuevos actores y temas en la agenda, y los nuevos canales de comunicación empiezan a preponderar en la formulación de política mundial. Sin embargo, se debe recalcar que esta teoría, creada por Robert Keohane y Joseph Nye, hace referencia especial al poder que los actores tienen en la toma de decisiones. De esta manera, nacen los conceptos de *hard power* y *soft power* para diferenciar las formas de poder, y que amplía los contextos en los que se usan los mismos. Después de los ataques terroristas del 9/11 y las políticas represivas e invasivas que se aplicaron en la Política Exterior estadounidense durante el mandato de George W. Bush, el gobierno de Barack Obama adopta el concepto de *smart power* como estrategia para utilizar ambos poderes de manera equilibrada y recuperar la hegemonía dentro del sistema internacional.

- La globalización también trajo cambios dentro la comunicación, que se incrementó y facilitó gracias a la invención del internet. Esta dio paso a la Era de la Información, período referente al desarrollo de la tecnología que influyó incluso en la política mundial. El ciberespacio se convirtió en un nuevo dominio, el cual posee una naturaleza cambiante, y por lo cual ejercer poder dentro del mismo se ha convertido en una tarea compleja para los Estados, los cuales se ven invadidos por múltiples actores que poseen mayores ventajas. Por lo tanto, las vulnerabilidades del Estado aumentan y sus fallas de seguridad son perceptibles frente a otros actores. Se toma el caso de Edward Snowden, el cual vulneró y filtró información clasificada de las tácticas de espionaje de Estados Unidos, que a su vez no tuvo capacidad de reacción inmediata frente a las fallas presentes.

- La Era de la Información también afectó la relevancia de la misma, puesto que después de tres años, las revelaciones de Snowden han perdido influencia. Se puede inferir que estos sucesos se dan debido a la cantidad de información que se difunde. El 2013 se caracterizó por hacer una crítica a los programas de espionaje y los intereses ocultos detrás de las acciones

contra el terrorismo. Sin embargo, las guerras en Medio Oriente, la igualdad de género y derechos LGBTI, ataques terroristas constantes y la luchas contra la violencia provocada por el machismo, han saturado y eclipsado los esfuerzos de Snowden de revelar la verdad. Lo que en un momento es controversial, al siguiente se ve desplazado por una nueva noticia.

- Por consiguiente, Estados Unidos continúa siendo el hegemón dentro del sistema internacional y dentro del ciberespacio en cuanto a influencia se refiere, puesto que sus recursos son mayores que cualquier otro país, y ciertamente que un individuo. Puede que este actor sea vulnerable frente a actores no estatales en temas de seguridad, pero domina los siete puntos estratégicos del ciberespacio. Estos están relacionados con la información que se difunde en internet, el medio de comunicación más efectivo en la actualidad. Estados Unidos es capaz de censurar, publicar o manipular el orden de relevancia de la información al momento de realizar una búsqueda en internet, dado que las empresas de esta nacionalidad predominan en el segundo punto estratégico: los motores de búsqueda. Hay que mencionar, además que Estados Unidos, mediante las empresas de infraestructura, sistema operativo, almacenamiento virtual y encriptación y protocolo, ejerce una influencia mundial, lo cual representa seis de los puntos estratégicos.

- WikiLeaks y Snowden crearon una tendencia a nivel mundial: la transparencia. Esta tomó un papel importante dentro de la política mundial, pues legitima las acciones de un Estado. De acuerdo con esta afirmación, la Agencia Nacional de Seguridad estadounidenses (NSA) publicó los documentos filtrados por Snowden y desclasificó las sentencias de los juicios del Tribunal de Vigilancia de Inteligencia Extranjera (FISC). De la misma manera, la agencia reveló las tácticas utilizadas para la obtención de metadatos y las empresas que fueron parte del espionaje. Finalmente, se incluyó en política exterior, leyes y en las estrategias del ciberespacio del 2015, el compromiso del gobierno con la transparencia.

- Snowden también demostró al mundo que Estados Unidos utiliza un doble discurso ya que las políticas y leyes, así como las declaraciones de los presidentes resaltan el compromiso que existe con la protección y respeto hacia la privacidad de los ciudadanos. Pese a esto, Estados Unidos es el autor principal de los espionajes a nivel mundial y ataques cibernéticos, que han sido tomados como medidas contra el terrorismo, pero que también han sido beneficiosos en temas económicos y políticos.

- En cuanto a la metodología utilizada en el trabajo de investigación, se aplicó un análisis cualitativo que realiza un enfoque profundo en la teoría, puesto que esta surge de académicos estadounidenses, los cuales influyen en la política del gobierno de Obama, además describen los fenómenos del ciberespacio. Dentro del segundo capítulo, se describe el caso de Snowden, haciendo un preámbulo sobre los sucesos de WikiLeaks que introduce las leyes que rigen durante caso principal, además dan una explicación de las motivaciones de Estados Unidos para legalizar os programas de vigilancia. Finalmente, se realiza un análisis, donde se conjuga la teoría con el caso, y se concluye que este proceso tiene relación con el tema investigado ya que resalta la importancia de la teoría, la cual es desarrollada bajo un enfoque estadounidense que encaja con el caso propuesto. Mediante la metodología utilizada, se logró examinar a profundidad las repercusiones en la hegemonía de Estados Unidos. Sin embargo, la metodología presenta limitaciones al momento de la elección de los documentos puesto que, refiriéndose al tema, la información es cuantiosa y sesgada a modelos estadounidenses, en ciertos casos.

VIII. RECOMENDACIONES

- La globalización y el rápido desarrollo tecnológico han permitido considerar a la tecnología y al ciberespacio como herramientas indispensables para la realización de las actividades cotidianas. Sin embargo, su rápida evolución no ha permitido considerarlas herramientas para adquirir poder o incluso un arma, la cual puede causar daños similares a las armas físicas. Por lo tanto, la necesidad de legislar su uso e implementar dentro del sistema educativo un espacio para el aprendizaje de los mismos. Además, por ese desarrollo acelerado, existen vacíos de conocimiento del ciberespacio, como el *dark web*, por lo tanto, es necesario ampliar los estudios que exploren este nuevo dominio.

- El surgimiento de nuevos actores en el sistema internacional trajo nuevos desafíos para los cuales los Estados no estaban preparados debido a la descentralización del poder. Más aún no comprenden el rol que estos desempeñan en la formulación de la política mundial y subestiman su poder. Los Estados, como actores que durante siglos monopolizaron el poder, no comprenden en su totalidad que las tácticas de ejercer influencia en la sociedad han cambiado, y que el uso de la fuerza no es el medio adecuado para lograr sus objetivos. Por lo tanto, es importante empezar a considerar a los individuos como actores que pueden provocar un cambio, y profundizar su estudio en cuanto a las motivaciones, objetivos e intereses, así como a las implicaciones de su accionar en el sistema internacional para poder comprender el rol que podrían desarrollar en un futuro. Cabe recalcar que son los individuos los que detectan las puertas traseras de los sistemas computacionales y deberían ser los primeros en ser captados como potenciales asesores para el perfeccionamiento de las redes.
  .

- La teoría del *smart power* todavía necesita de desarrollo, puesto que presenta muchas fallas metodológicas, desde su concepción. Sin embargo, como señala Joseph Nye, la clave para un eficiente desarrollo, es la inteligencia contextual, la cual está basada en la habilidad de ciertos líderes para tomar decisiones en momentos cruciales. Existe todavía una falta de consenso entre los actores, en cuanto a las leyes internacionales que regulan el ciberespacio. Los crímenes que se cometen a nivel físico causan pérdidas económicas, desestabilización política, llegando a crear guerras. Por lo tanto, al espionaje a través de la red, así como cualquier crimen que se cometa en el ciberespacio, debe ser considerado con la misma severidad que otros crímenes, lo cual se logra a través de la cooperación internacional.

- Se recomienda para la aplicación de la metodología cualitativa que la información a utilizar haya pasado por un procedimiento de selección que permita determinar la relevancia y esté centrado en los detalles. De la misma manera, la utilización de dos metodologías contribuiría a respaldar la premisa inicial, siempre que el tema lo requiera.

IX. LISTA DE REFERENCIAS

Libros

Brown, L. R. (1972). *World Without Borders: The Interdependence.* Nueva York: Foreign Policy Association

Kuehl, D. T. (2014). *From Cyberspace to Cyberpower: Defining the Problem.* Obtenido de Center for Technology and National Security Policy: http://ctnsp.dodlive.mil/files/2014/03/Cyberpower-I-Chap-02.pdf

Morgenthau, H. (1948). Política entre las Naciones. La Lucha por el poder y la paz. New York: McGraw Hill.

National Academy of Engineering. (1992). *Time Horizons and Technology Investments.* Washington: National Academy Press. Obtenido de The National Academy of Engineering: https://www.nap.edu/read/1943/chapter/7

Nye, J. (2003). *La paradoja del poder norteamericano.* Madrid: Santillana.

Nye, J. (1990). Soft Power. *Foreign Policy*, 153-171.

Nye, J. (2011). *The Future of Power.* New York: Public Affairs.

Waltz, K. (1979). *Teoría de la Política Internacional.* McGraw Hill.

Publicaciones

Amnistía Internacional. (2015). *Dos años después de Snowden: proteger los derechos humanos en una era de vigilancia masiva*. Obtenido de Amnistía Internacional: https://amnistia.org.ar/wp-content/uploads/delightful-downloads/2017/03/ACT3017952015SPANISH.pdf

ANSA y DPA. (03 de Junio de 2015). *EE.UU.: aprueban la nueva ley de espionaje.* Obtenido de La Nación: http://www.lanacion.com.ar/1798196-eeuu-aprueban-la-nueva-ley-de-espionaje

BBC. (26 de Agosto de 2010). *El día que un ataque cibernético amenazó a EE.UU.* Obtenido de BBC Mundo: http://www.bbc.com/mundo/internacional/2010/08/100826_1400_eeuu_internet_virus_ciberataque_lynn_dc

Bejarano, M. J. (29 de Mayo de 2013). *Poder blando frente a poder duro en el ciberespacio.* Obtenido de Instituto Español de studios Estratégicos: http://www.ieee.es/Galerias/fichero/docs_analisis/2013/DIEEEA33-2013_PoderDuroPoderBlandoEnCiberespacio_MJCB.pdf

Brown, H. (18 de Diciembre de 2014). *Good Question: How Often Do Hackers Get Caught?* Obtenido de CBS: http://minnesota.cbslocal.com/2014/12/18/good-question-how-often-do-hackers-get-caught/

Byman, D. y. (Mayo/Junio de 2014). *Reforming the NSA: How to Spy after Snowden*. Obtenido de Foreign Affairs: http://www.foreignaffairs.com/articles/141215/daniel-byman-and-benjamin-wittes/reforming-the-nsa

Carrasco, L. d. (Diciembre de 2010). *Internet, Filtraciones y WikiLeaks.* Obtenido de Instituto Español de Estudios Estratégicos: http://www.ieee.es/Galerias/fichero/docs_opinion/2010/DIEEEO25_2010Wikileaks.pdf

Clemente, D. (Febrero de 2013). *Cyber Security and Global Interdependence: What is Critical?* Obtenido de Chatam House: https://www.chathamhouse.org/sites/files/chathamhouse/public/Research/International%20Security/0213pr_cyber.pdf

Coto, M. V. (2012). *¿Poder inteligente? La Doctrina Obama y Guantánamo.* Obtenido de Aportes Teóricos de Nuestra América: http://www.alainet.org/images/PoderInteligente.pdf

Fink, A. (Noviembre de 2010). *Acerca del concepto de seguridad.* Obtenido de Quinto Congreso de Relaciones Internacionales: https://www.iri.edu.ar/publicaciones_iri/IRI%20COMPLETO%20-%20Publicaciones-V05/Publicaciones/cd%20V%20congreso/ponencias/0%20Fink_Acerca%20del%20concepto%20de%20seguridad.pdf

Gallagher, R. &. (12 de Marzo de 2014). *How the NSA plans to infect "millions" of computers with Malware.* Obtenido de The Intercept: https://theintercept.com/2014/03/12/nsa-plans-infect-millions-computers-malware/

Gao, G. (29 de Mayo de 2015). *What Americans think about NSA surveillance, national security and privacy.* Obtenido de Pew Research Center: http://www.pewresearch.org/fact-tank/2015/05/29/what-americans-think-about-nsa-surveillance-national-security-and-privacy/

González, F. J. (13 de Septiembre de 2011). *Tendencias y dilemas internacionales tras el 11-s de 2001: ¿un sistema internacional en transición?* Obtenido de Instituto Español de Estudios Estratégico: http://www.ieee.es/Galerias/fichero/docs_analisis/2011/DIEEEA23-2011_TENDENCIAS_Y_DILEMAS_TRAS_EL_11-S.pdf

Greenwald, G. E. M. (11 de Junio de 2013). *Edward Snowden: the whistleblower behind the NSA surveillance revelations.* Obtenido de The Guardian: https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance

Greenwald, G. (24 de Febrero de 2014). *How covert agents infiltrate the internet to manipulate, deceive and destroy reputations.* Obtenido de The Intercept: https://theintercept.com/2014/02/24/jtrig-manipulation/

Greenwald, J. S. (10 de Febrero de 2014). *The NSA secret role in the U.S. assassination program.* Obtenido de The Intercept: https://theintercept.com/2014/02/10/the-nsas-secret-role/

Kayyali, D. (07 de Mayo de 2014). *The Way the NSA Uses Section 702 is Deeply Troubling. Here's Why.* Obtenido de Electronic Frontier Foundation: https://www.eff.org/deeplinks/2014/05/way-nsa-uses-section-702-deeply-troubling-heres-why

Levine, A. (29 de Julio de 2010). *Top military official: WikiLeaks founder may have 'blood' on his hands.* Obtenido de CNN News: http://edition.cnn.com/2010/US/07/29/wikileaks.mullen.gates/index.html

Lewis, J. A. (2014). *The Snowden Effect: Can we undo the damage to american power?* Obtenido de Global Forecast : https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/131112_chap2_Lewis.pdf

Miles, T. (15 de Julio de 2013). *Snowden affair is chance for truce in cyber war: U.N.* . Obtenido de Reuters: http://www.reuters.com/article/2013/07/15/net-us-usa-security-cybertruce-idUSBRE96E0L320130715

NPR. (20 de Septiembre de 2013). *The Effects Of The Snowden Leaks Aren't What He Intended.* Obtenido de National Press Radio: http://www.npr.org/2013/09/20/224423159/the-effects-of-the-snowden-leaks-arent-what-he-intended

O'Neill, B. (22 de Febrero de 2014). *FISA, the NSA, and America's Secret Court System.* Obtenido de Mises Daily Articles: https://mises.org/library/fisa-nsa-and-america%E2%80%99s-secret-court-system

Peterson, A. (Diciembre de 2014). *The Sony Pictures hack, explained*. Obtenido de The Washington Post: https://www.washingtonpost.com/news/the-switch/wp/2014/12/18/the-sony-pictures-hack-explained/?utm_term=.9ec08c556756

Pew Research Center. (2014). *Chapter 1: The American Brand.* Obtenido de Pew Research Center: http://www.pewglobal.org/2014/07/14/chapter-1-the-american-brand/

Pew Research Center. (14 de Julio de 2014). *Global Opposition to U.S. Surveillance and Drones, but Limited Harm to America's Image.* Obtenido de Pew Research Center: http://www.pewglobal.org/2014/07/14/global-opposition-to-u-s-surveillance-and-drones-but-limited-harm-to-americas-image/

Poushter, J. (29 de Junio de 2016). *Key takeaways on international image of the U.S., Obama and presidential candidates.* Obtenido de Pew Research Center: http://www.pewresearch.org/fact-tank/2016/06/29/key-takeaways-us-image/

Rainie, L. (21 de Septiembre de 2016). *The state of privacy in post-Snowden America.* Obtenido de Pew Research Center: http://www.pewresearch.org/fact-tank/2016/09/21/the-state-of-privacy-in-america/

Reitman, C. C. (2 de Junio de 2015). *USA Freedom Act Passes: What We Celebrate, What We Mourn, and Where We Go From Here*. Obtenido de Electronic Frontier Foundation: https://www.eff.org/deeplinks/2015/05/usa-freedom-act-passes-what-we-celebrate-what-we-mourn-and-where-we-go-here

Semana. (29 de Noviembre de 2014). *El espionaje ruso en el mundo.* Obtenido de Semana: http://www.semana.com/mundo/articulo/el-espionaje-ruso-en-el-mundo/410748-3

Simcox, R. (2015). *Surveillance after Snowden.* Obtenido de Henry Jackson Society: http://henryjacksonsociety.org/wp-content/uploads/2015/06/Surveillance-After-Snowden-16.6.15.pdf

Snowden, E. (9 de Julio de 2013). NSA whistleblower Edward Snowden: 'I don't want to live in a society that does these sort of things'. (G. Grindewald, Entrevistador) Obtenido de The Guardian: https://www.youtube.com/watch?v=0hLjuVyIIrs

Tamayo, E. (Julio de 2013). *Espionaje global de EE.UU.* Obtenido de Alainet: https://www.alainet.org/es/active/65377#_ftnref9

The Economist. (25 de Febrero de 2010). *Data, data everywhere.* Obtenido de The Economist: http://www.economist.com/node/15557443

The Guardian. (22 de Mayo de 2016). *How the Pentagon punished NSA whistleblowers.* Obtenido de The Guardian:

https://www.theguardian.com/us-news/2016/may/22/how-pentagon-punished-nsa-whistleblowers

The Statistics Portal. (Agosto de 2016). *Global market share of cloud infrastructure services as of the second quarter 2016, by vendor*. Obtenido de The Statistics Portal: https://www.statista.com/statistics/477277/cloud-infrastructure-services-market-share/

The Statistics Portal. (2017). *Biggest cyber security problems facing the U.S. government according to adults in the United States as of January 2017.* Obtenido de The Statistics Portal: https://www.statista.com/statistics/676601/biggest-us-government-cyber-security-problems/

The Statistics Portal. (Mayo de 2017). *Global industries most targeted by cyber espionage in 2016.* Obtenido de The Statistics Portal: https://www.statista.com/statistics/221293/cyber-crime-target-industries/

The Statistics Portal. (Agosto de 2017). *Global mobile OS market share in sales to end users from 1st quarter 2009 to 2nd quarter 2017*. Obtenido de The Statistics Portal: https://www.statista.com/statistics/266136/global-market-share-held-by-smartphone-operating-systems/

The Statistics Portal. (Julio de 2017). *Global operating systems market share for desktop PCs, from January 2013 to July 2016*. Obtenido de The Statistics Portal: https://www.statista.com/statistics/218089/global-market-share-of-windows-7/

The Statistics Portal. (2017). *U.S. government and cyber crime - Statistics & Facts.* Obtenido de The Statistics Portal: https://www.statista.com/topics/3387/us-government-and-cyber-crime/

The Washington Post. (2 de Junio de 2015). *USA Freedom Act: What's in, what's out*. Obtenido de The Washington Post: https://www.washingtonpost.com/graphics/politics/usa-freedom-act/

THIBER. (11 de Noviembre de 2013). *La Agencia de Seguridad Nacional (NSA), el espionaje y colaboración público-privada en EEUU.* Obtenido de Real Instituto Elcano: http://www.realinstitutoelcano.org/wps/portal/rielcano_es/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_es/zonas_es/defensa+y+seguridad/ari41-2013-thiber-nsa-espionaje-colaboracion-publico-privada-snowden

Winnett, R. (30 de Julio de 201). *Wikileaks Afghanistan: Taliban 'hunting down informants.* Obtenido de The Telegraph: http://www.telegraph.co.uk/news/worldnews/asia/afghanistan/7917955/Wikileaks-Afghanistan-Taliban-hunting-down-informants.html

World Economic Forum. (10 de Marzo de 2017). *Las 10 mayores economías del mundo en 2017*. Obtenido de https://www.weforum.org/es/agenda/2017/03/las-10-mayores-economias-del-mundo-en-2017/

Revistas

Acevedo, N. M. (2013). Cambios es la estructura de poder: interdependencias y asimetrías en la era global. *Papel político*, 677-699.

Brown, L. R. (1972). *World Without Borders: The Interdependence.* Nueva York: Foreign Policy Association.

Gupta, S. K. (s/f). *Extradition Law and the International Criminal.* Obtenido de Berkeley Journal of Criminal Law: https://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=1072&context=bjcl

Herrington, W. C. (2015). *"Snowed In" in Russia: A Historical Analysis of American and Russian Extradition and How the Snowden Saga Might Impact the Future.* Obtenido de Journal of Law and Policy: http://openscholarship.wustl.edu/law_journal_law_policy/vol48/iss1/16

Keohane & Nye, R. J. (1977). *Poder e interdependencia. La política mundial en transición.* Buenos Aires: Grupo Editor Latinoamericano. Obtenido de Jstor: http://www.jstor.org/stable/20049052?seq=1#page_scan_tab_contents

Keohane, R. O. (1984). *After Hegemony: Cooperation and Discord in the World Political Economy.* New Jersey: Princeton Uiversity Press.

Nye y Armitage, J. &. (2007). A smarter more secure America. *Center for Strategic and International Studies*, 17 - 60.

Nye, J. (2004). *El poder blando y la política exterior americana.* Obtenido de Public Affairs: http://www.relacionesinternacionales.info/ojs/article/view/218.html

Nye, J. (2009). *Get Smart: Combining Hard and Soft Power.* Obtenido de Foreign Affairs, 88(4), pp. 160-163: http://www.jstor.org/stable/20699631

Nye, J. (2010). *Cyber Power.* Cambridge: Belfer Center for Science and International Affairs.

Nye, J. (13 de Abril de 2012). *Joseph S. Nye: Cyber War and Peace.* Obtenido de The Strait Times: http://www.straitstimes.com/world/joseph-s-nye-cyber-war-and-peace

Popa, I. F. (Enero de 2015). *Extensive Transparency as a Principle of Cyberspace Governance and Cyber Security Dilemma Prevention.* Obtenido de Letter and Social Science Series: http://www.utgjiu.ro/revista/lit/pdf/2015-01/10_Popa.pdf

Rana, W. (February de 2015). *Theory of Complex Interdependence: A Comparative Analysis of Realist and Neoliberal Thoughts.* Obtenido de International Journal of Business and Social Science : http://ijbssnet.com/journals/Vol_6_No_2_February_2015/33.pdf

Rieff, D. (22 de Agosto de 2013). *Why Nobody Cares About the Surveillance State.* Obtenido de Foreign Policy: http://foreignpolicy.com/2013/08/22/why-nobody-cares-about-the-surveillance-state/

Santana, D. H. (enero-abril de 2017). *Hegemonía y Relaciones Internacionales.* Obtenido de Revistas UNAM: http://www.revistas.unam.mx/index.php/rri/article/viewFile/61145/53941

Sonenshine, T. D. (2015). *Is "smart power" smart and does it work?* Obtenido de Contemporary Smart Power: http://publicdiplomacymagazine.com/wp-content/uploads/2015/06/Smart-Power-PD-Mag.pdf

Web

Banco Mundial. (2016). Estados Unidos. Obtenido de Banco Mundial: https://datos.bancomundial.org/pais/estados-unidos

IMPACT. (s.F). *About us.* Obtenido de IMPACT: http://www.impact-alliance.org/aboutus/mission-&-vision.html

NSA. (2014). *Utah Data Center*. Obtenido de Domestic Surveillance Directorate: https://nsa.gov1.info/utah-data-center/

NSA. (s.F.). *Surveillance*. Obtenido de National Segurity Agency: https://nsa.gov1.info/surveillance/

OTAN. (s.F.). *Nuevas amenazas: el ciberespacio.* Obtenido de Revista de la OTAN: http://www.nato.int/docu/review/2011/11-september/Cyber-Threads/ES/index.htm

WikiLeaks. (s.F.). *About*. Obtenido de WikiLeaks: https://wikileaks.org/What-is-Wikileaks.html

Informes

Budapest Conference. (4 y 5 de Octubre de 2012). *Budapest Conference*. Obtenido de Global Command and Control System: https://www.gccs2015.com/sites/default/files/documents/Chair%27s%20Summary%20Budapest.pdf

Convención de Budapest. (23 de Noviembre de 2001). *Convenio sobre la Ciberdelicuencia.* Obtenido de Organización de Estados Americanos (OAS): https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

Council of Europe. (18 de Diciembre de 2014). *Convention on Cybercrime.* Obtenido de Council of Europe: http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG

Department of Defense. (Julio de 2011). *Department of Defense Strategy for Operating in Cyberspace.* Obtenido de Department of Defense: http://csrc.nist.gov/groups/SMA/ispab/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf

Department of Energy. (Marzo de 2018). *Strategic Plan 2014 - 2018*. Obtenido de U.S. Department of Energy: https://www.energy.gov/sites/prod/files/2014/04/f14/2014_dept_energy_strategic_plan.pdf

Department of Homeland Security. (2009). *Cyberspace Policy Review* . Obtenido de Department of Homeland Security: https://www.dhs.gov/sites/default/files/publications/Cyberspace_Policy_Review_final_0.pdf

Department of Homeland Security. (2010). *Cyberspace Policy Review.* Obtenido de Department of Homeland Security: https://www.dhs.gov/sites/default/files/publications/Cyberspace_Policy_Review_final_0.pdf

Department of Homeland Security. (2015). *Cybersecurity Information Sharing Act of 2015*. Obtenido de Federal Privacy Council: https://www.fpc.gov/19081

IISS. (2016). *Top 15 defense Budget*. Obtenido de International Institute for Strategic Studies: https://www.iiss.org/en/publications/military%20balance/issues/the-military-balance-2015-5ea6

Kissinger, H. (17 de Febrero de 1975). *A New National Partnership.* Obtenido de Department of State Bulletin:

https://www.fordlibrarymuseum.gov/library/document/dosb/1860.pdf#page=3

Lugo, D. (14 de Febrero de 2003). *Estrategia Nacional para Combatir el Terrorismo.* Obtenido de InterAmerican Affairs - International Division: http://interamerican-usa.com/articulos/Crim-org-terr/Estr-Antiterr.htm

Maude, F. (4 de Octubre de 2012). *Budapest Conference on Cyberspace 2012.* Obtenido de UK Goverment: https://www.gov.uk/government/speeches/budapest-conference-on-cyberspace-2012

Nye & Armitage, J. R. (2007). A smarter, more secure America. Obtenido de Center for Strategic and International Studies: https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/media/csis/pubs/071106_csissmartpowerreport.pdf

Obama, B. (29 de Mayo de 2009). *Remarks by the President on Securing Our Nation's Cyber Infrastructure.* Obtenido de The White House: https://obamawhitehouse.archives.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure

Obama, B. (27 de Julio de 2010). Obama on WikiLeaks: I'm Concerned. (CNN, Entrevistador)

Seger, A. (16 de Febrero de 2012). *The Budapest Convention on Cybercrime 10 years on: Lessons learnt or the web is a web.* Obtenido de Council of Europe: https://rm.coe.int/16802fa3e0

The White House. (Febrero de 2015). *Executive Order 13691 - Promoting Private Sector Cybersecurity Information Sharing.* Obtenido de Federal Privacy Programs: https://www.fpc.gov/19081/

U.S. Army Cyber Command. (s.F). *U.S. Cyber Command*. Obtenido de U.S. Army Cyber Command: http://www.arcyber.army.mil/Pages/USCyberCommand.aspx

UIT. (2014). *Resolution 130.* Obtenido de Unión Internacional de Telecomunicaciones: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/130revBusan.pdf

UIT. (s/f). *Sobre la Unión Internacional de Telecomunicaciones (UIT).* Obtenido de Unión Internacionalde Teleomunicaciones: https://www.itu.int/es/about/Pages/default.aspx

UKUSA Agreement. (3 de Mayo de 2016). *UKUSA Agreement Release.* Obtenido de National Security Agency: https://www.nsa.gov/news-features/declassified-documents/ukusa/

Audiovisual

Kirk, M. (Dirección). (2014). *United States of Secrets* [Película].

Disertaciones

Arenal, C. (2009). *Mundialización, creciente interdependencia y globalización en las Relaciones Internacionales.* Obtenido de Universidad Complutense de Madrid: http://www.ehu.eus/cursosderechointernacionalvitoria/ponencias/pdf/2008/2008_4.pdf

Creus, N. (2013). *El concepto de poder en las relaciones internacionales y la necesidad de incorporar nuevos enfoques.* Obtenido de Revista de Estudios Internacionales de la Universidad de Chile: http://www.revistaei.uchile.cl/index.php/REI/article/viewFile/27372/30150

Havrylenko, I. (2015). *U.S. Smart Power in International Relations.* Obtenido de Taras Shevchenko National University of Kyiv: http://eppd13.cz/wp-content/uploads/2015/2015-2-2/13.pdf

Lopez, D. Z. (Agosto de 2012). *WikiLeaks y los efectos de la divulgación de información confidencial: análisis de las filtraciones de Estados Unidos.* Obtenido de Biblioteca Rafael Montejano y Aguiñaga: http://biblio.colsan.edu.mx/tesis/ZacariasLopezDaniela.pdf

López, S. M. (20 de Junio de 2014). *Programas de Vigilancia de Internet*. Obtenido de Universitat Oberta de Catalunya: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/36661/6/smartinloTFM0614memoria.pdf

Lundberg, K. (Junio de 2011). *Friend or Foe? WikiLeaks and the Guardian.* Obtenido de The Journalism School Knight Case Studies Iniciative : http://ccnmtl.columbia.edu/projects/caseconsortium/casestudies/70/casestudy/files/global/70/WikiLeaks%20and%20the%20Guardian.pdf

Mamritsova, D. (5 de Enero de 2018). *The digital panopticon: media, state and cultural hegemony in the case of the revelations made by Edward Snowden.* Obtenido de Universiteit Leiden : https://openaccess.leidenuniv.nl/bitstream/handle/1887/57777/LUthesisruDM.pdf?sequence=1

Sauceda, J. B. (enero-junio de 2015). *Cultura de paz y resolución de conflictos: la importancia de la mediaciónen la construcción de un estado de paz*. Obtenido de Universidad Autónoma Indígena de México: http://www.redalyc.org/pdf/461/46139401006.pdf

Stone, R. W. (Agosto de 2008). *Institutions, Power, and Interdependence* . Obtenido de University of Rochester: http://www.sas.rochester.edu/psc/stone/book_chapters/princeton_2009.pdf

Yoon, J. M. (2015). *Edward Snowden, Criminal or Patriot: Media Coverage of National Security Agency Document Leaks.* Obtenido de Andrews University: https://digitalcommons.andrews.edu/cgi/viewcontent.cgi?article=1115&context=honors

ANEXOS

ANEXO 1
U.K - U.S. COMMUNICATIONS INTELLIGENCE AGREEMENT (UKUSA AGREEMENT)

TOP SECRET
TO BE HANDLED IN ACCORDANCE WITH IRSIG

EIDER

U.K. - U.S. COMMUNICATIONS INTELLIGENCE

AGREEMENT (UKUSA AGREEMENT)

1. Parties to the Agreement

The following agreement is made between the United States Communications Intelligence Board (USCIB) (formerly known as STANCIB, representing the U.S.) and the London Signal Intelligence Board (LSIB) (representing the U.K.).

2. Scope of Agreement

The agreement governs the relations of the above-mentioned parties in communications intelligence (hereinafter referred to as COMINT) matters only. However the exchange of such collateral material as is applicable for technical purposes and is not prejudicial to national interests will be effected between the National Communication Intelligence Agencies of both countries.

3. Appendices to the Agreement

Certain terms used in the Agreement are defined in Appendix A. Additional documents are appended for the purpose of clarifying the agreement, stating the principles of COMINT security, and otherwise guiding or governing the collaboration between the two countries in COMINT matters. The appendices are described more fully in an introduction to the appendices (attached hereto).

4. Extent of the Agreement - Products

(a) The parties agree to the exchange of the products of the following operations relating to foreign communications:-

(1) Collection of traffic.

(2) Acquisition of communications documents and equipment.

(3) Traffic analysis.

(4) Cryptanalysis.

(5) Decryption and translation.

(6) Acquisition of information regarding communications organizations, procedures, practices and equipment.

/(b)

(b) Such exchange will be unrestricted on all work undertaken except when specifically excluded from the agreement at the request of either party and with the agreement of the other. It is the intention of each party to limit such exceptions to the absolute minimum and to exercise no restrictions other than those reported and mutually agreed upon.

5. Extent of the Agreement - Methods and Techniques

(a) The parties agree to the exchange of information regarding methods and techniques involved in the operations outlined in paragraph 4(a).

(b) Such exchange will be unrestricted on all work undertaken except that upon notification of the other party information may be withheld by either party when its special interests so require. Such notification will include a description of the information being withheld, sufficient in the opinion of the withholding party, to convey its significance. It is the intention of each party to limit such exceptions to the absolute minimum.

6. Third Parties to the Agreement

Both parties will regard this agreement as precluding action with third parties on any subject appertaining to COMINT except in accordance with the following understanding:-

(a) It will be contrary to this Agreement to reveal its existence to any third party unless otherwise agreed by the two parties.

(b) Except as laid down in Appendix P, each party will seek the agreement of the other to actions with third parties, and will take no such action until its advisability is agreed upon.

(c) The agreement of the other having been obtained, it will be left to the party concerned to carry out the agreed action in the most appropriate way, without obligation to disclose precisely the channels through which action is taken.

/(d)

(d) Each party will ensure that the results of any of its actions with third parties are made available to the other.

7. Commonwealth Countries other than the U.K.

(a) While Commonwealth Countries other than the U.K. are not parties to this agreement, they will not be regarded as third parties.

(b) LSIB will keep USCIB informed of any arrangements or proposed arrangements with other Commonwealth COMINT Authorities.

(c) USCIB will make no arrangements in the sphere of COMINT with any Commonwealth COMINT Authorities other than Canadian, except through, or with the prior approval of, LSIB.

(d) As regards Canada, USCIB will complete no arrangements with any COMINT Authority therein, without first obtaining the views of LSIB.

(e) It will be conditional on any Commonwealth Authorities with whom collaboration takes place that they abide by the terms of paragraphs 6, 9 and 10 of this agreement and by the arrangements laid down in paragraph 8.

8. Arrangements between LSIB and U.S. Authorities and USCIB and U.K. Authorities

(a) LSIB will make no arrangements in the sphere of COMINT with any U.S. authority except through, or with prior approval of, USCIB.

(b) USCIB will make no arrangements in the sphere of COMINT with any U.K. authority except through, or with prior approval of, LSIB.

9. Dissemination and Security

Classified COMINT information and materials will be disseminated and safeguarded in accordance with principles drawn up and kept under review by USCIB and LSIB in collaboration. These principles shall be the basis for all regulations on this subject issued by or under the authority of USCIB or LSIB and other appropriate authorities of the Governments of the two parties. Within the terms of these regulations dissemination by either party will be made to U.S.

recipients only as approved by USCIB; to Commonwealth recipients other than Canadian, only as approved by LSIB; to Canadian recipients only as approved by either USCIB or LSIB; and to third party recipients only as jointly approved by USCIB and LSIB as provided in Appendix P.

10. Dissemination and Security - Commercial

USCIB and LSIB will ensure that without prior notification and consent of the other party in each instance no dissemination of information derived from COMINT sources is made to any individual or agency, governmental or otherwise, that will exploit it for commercial purposes.

11. Previous Agreements

This Agreement supersedes all previous Agreements between U.K. and U.S. authorities in the COMINT field.

12. Amendment and Termination of Agreement

This Agreement may be amended or terminated completely or in part at any time by mutual agreement. It may be terminated completely at any time on notice by either party, should either consider its interests best served by such action.

13. Activation and Implementation of Agreement

This Agreement becomes effective by signature of duly authorized representatives of the parties. Thereafter, its implementation will be arranged between the COMINT authorities concerned subject to the approval of LSIB and USCIB.

For and in behalf of the
London Signal Intelligence Board

For and in behalf of the United States
Communications Intelligence Board

/Introduction to

Fuente: (UKUSA Agreement, 2016)