**PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR**
**FACULTAD DE COMUNICACIÓN, LINGÜÍSTICA Y LITERATURA**
**ESCUELA MULTILINGÜE EN NEGOCIOS Y RELACIONES INTERNACIONALES**

**TRABAJO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE LICENCIADO MULTILINGÜE EN NEGOCIOS Y RELACIONES INTERNACIONALES**

# ANÁLISIS DE LAS REPERCUSIONES DEL SURGIMIENTO DE WIKILEAKS COMO UN ACTOR TRANSNACIONAL EN LAS RELACIONES INTERNACIONALES Y SU INFLUENCIA EN LA CREACIÓN DE POLÍTICAS Y AGENCIAS DE CIBERSEGURIDAD QUE AFECTARON EN EL AUMENTO DE LA HEGEMONÍA ESTADOUNIDENSE DURANTE EL PERÍODO 2010-2015

**JESSICA PAMELA TORRES**

**DIRECTORA:**

**DRA. GILDA GUERRERO**

**Octubre, 2020**
**QUITO – ECUADOR**

“The internet has become a political space. I think that is one of the most important developments in the past decade.”

— Julian Assange

*Agradecimientos:*

*A mis padres, Elio y Eliza por su inquebrantable apoyo y esfuerzo en todas las etapas de mi vida, además de ser mi guía y mi motivación en todo lo que me he propuesto y porque han sido un pilar fundamental en mi crecimiento personal y profesional.*

*A mis hermanos por apoyarme siempre*

*Doy gracias a. Dios por la bendición de tenerlos como familia*

*A mi directora de tesis, Gilda Guerrero, por ser mi guía, darme su tiempo y dedicación durante este largo proceso y por ser una excepcional profesora que por medio de su conocimiento en sus clases ha inspirado a aprender y ver más allá de lo establecido.*

*A mis amigos que me han estado incondicionalmente dándome ánimo*

*A mis mascotas Kin y Estrellita por acompañarme en mis largas noches de desvelo*

## ÍNDICE DE CONTENIDO

## ÍNDICE DE TABLAS

## ÍNDICE DE ANEXOS

## I. TEMA

**ANÁLISIS DE LAS REPERCUSIONES DEL SURGIMIENTO DE WIKILEAKS COMO UN ACTOR TRANSNACIONAL EN LAS RELACIONES INTERNACIONALES Y SU INFLUENCIA EN LA CREACIÓN DE POLÍTICAS Y AGENCIAS DE CIBERSEGURIDAD QUE AFECTARON EN EL AUMENTO DE LA HEGEMONÍA ESTADOUNIDENSE DURANTE EL PERÍODO 2010-2015**

## II. RESUMEN

La globalización en los últimos años ha traído grandes cambios innegables en la sociedad los cuales son importantes, debido a que han impulsado nuevas interacciones sociales, culturales, políticas y económicas en todo el mundo. La creación del internet ha marcado el inicio de una nueva era moderna en donde el ciberespacio se ha convertido en un lugar abierto de interacción virtual para diferentes actores, en donde tienen la posibilidad de empoderarse y ejercer acciones de todo tipo. Es por esto, que la presente investigación se enfoca en este contexto moderno del ciberespacio, el cual brinda la apertura a nuevos actores transnacionales como lo es la organización WikiLeaks, la cual se destacó por ejecutar acciones que tenían la intención de llegar a ser desestabilizadoras o determinar un nuevo comportamiento de actores estatales principalmente. Este caso de estudio busca identificar las vulnerabilidades en la ciberseguridad de los Estados Unidos ante estas amenazas recientes y como estos sucesos protagonizados por las filtraciones de información confidencial por WikiLeaks durante el 2010 tuvieron un impacto en las políticas nacionales como en la política exterior con repercusión en las relaciones internacionales. Para llevar a cabo el análisis de esta investigación, la metodología empleada es la de análisis de contenido, en conjunto con el marco teórico que utilizó como base general la teoría de interdependencia compleja de Keohane y Nye, en combinación con escritos más recientes de Nye, sobre el poder blando y duro en la era tecnológica. Con estas

herramientas se pretende identificar si las acciones anti hegemónicas de WikiLeaks en el ciberespacio, provocaron la creación de políticas y agencias de ciberseguridad que fortalecieron a la hegemonía estadounidense en el período 2010-2015. En resumen, la hipótesis planteada para esta disertación se cumple parcialmente ya que, se encontró que la organización WikiLeaks no fue el actor principal que provocó grandes cambios en la creación de políticas y agencias de ciberseguridad en EE. UU, no obstante, si influyó en la creación de políticas para el control de la información confidencial dentro de las agencias del gobierno y aumentó la consciencia de estar preparados ante las amenazas que surgen en el ciberespacio.

**Palabras clave:** ciberespacio, globalización, ciberseguridad, actores transnacionales, información clasificada, ciberpoder, WikiLeaks, ciberpolíticas

## III. ABSTRACT

Globalization in recent years has brought undeniable great changes in society, which are important, because they have fostered new social, cultural, political and economic interactions around the world. The creation of the internet has marked the beginning of a new modern era in which cyberspace has become an open place of virtual interaction for different actors, where they have the possibility of empowering themselves and exercising actions of all kinds. For this reason, this research focuses on this modern context of cyberspace, which offers openness to new transnational actors such as the WikiLeaks organization, which stood out for executing actions that were intended to become destabilizing or determine a new behavior of state actors mainly. This case study seeks to identify cybersecurity vulnerabilities in the United States in the face of these recent threats and how these events led by the leaks of confidential information by WikiLeaks during 2010 had an impact on national policies and foreign policy with repercussions on international relations. To carry out the analysis of this research, the methodology used is that of content analysis, together with the theoretical framework that took as a general basis the complex interdependence theory of Keohane and Nye, in combination with more recent writings by Nye, about soft and hard power in the technological age. These tools are intended to identify whether WikiLeaks' anti-hegemonic actions in cyberspace led to the creation of cybersecurity policies and agencies that strengthened the US hegemony in the 2010-2015 period. In summary, the hypothesis raised for this dissertation is partially fulfilled, since it was found that the WikiLeaks organization was not the main actor that caused great changes in the creation of cybersecurity policies and agencies in the US, however, it did influence in the creation of policies for the control of confidential information within government agencies and increased awareness of being prepared for threats that arise in cyberspace.

**Keywords:** cyberspace, globalization, cybersecurity, transnational actors, classified information, cyberpower, WikiLeaks, cyber policies

## IV. ABSTRAKT

Die Globalisierung hat in den letzten Jahren unbestreitbar große Veränderungen in der Gesellschaft bewirkt, die wichtig sind, weil sie neue soziale, kulturelle, politische und wirtschaftliche Interaktionen auf der ganzen Welt gefördert haben. Die Schaffung des Internets hat den Beginn einer neuen modernen Ära markiert, in der der Cyberspace zu einem offenen Ort der virtuellen Interaktion für verschiedene Akteure geworden ist, wo sie die Möglichkeit haben, sich selbst zu stärken und Handlungen aller Art auszuüben. Aus diesem Grund konzentriert sich diese Forschung auf diesen modernen Kontext des Cyberspace, der Offenheit für neue transnationale Akteure wie die WikiLeaks-Organisation bietet, die sich durch die Durchführung von Aktionen auszeichnete, die destabilisierend werden oder ein neues Verhalten staatlicher Akteure vor allem bestimmen sollen. Diese Fallstudie zielt darauf ab, Schwachstellen in der Cybersicherheit in den Vereinigten Staaten angesichts dieser jüngsten Bedrohungen zu identifizieren und wie diese Ereignisse, die durch die Leckagen von vertraulichen Informationen von WikiLeaks im Jahr 2010 geführt hatten, Auswirkungen auf die nationale Politik und die Außenpolitik mit Auswirkungen auf die internationalen Beziehungen hatten. Um die Analyse dieser Forschung durchzuführen, wird die Methodik der Inhaltsanalyse verwendet, zusammen mit dem theoretischen Rahmen, der als allgemeine Grundlage die komplexe Interdependenztheorie von Keohane und Nye verwendet, in Kombination mit neueren Schriften von Nye, über Soft und Hard Power im technologischen Zeitalter. Mit diesen Tools soll ermittelt werden, ob WikiLeaks antihegemoniales Aktionen im Cyberspace zur Schaffung von Cybersicherheits-Policies und -Agenturen geführt hat, die die US-Hegemonie im Zeitraum 2010-2015 gestärkt haben. Zusammenfassend lässt sich sagen, dass die für diese Dissertation aufgestellte Hypothese teilweise erfüllt ist, da festgestellt wurde, dass die WikiLeaks-Organisation nicht der Hauptakteur war, der große Änderungen bei der Erstellung von Cybersicherheitsrichtlinien und -agenturen in den USA verursacht hat, jedoch Einfluss auf die

Erstellung hatte von Richtlinien zur Kontrolle vertraulicher Informationen innerhalb von Regierungsbehörden und zur Sensibilisierung für die Vorbereitung auf Bedrohungen, die im Cyberspace auftreten.

**Schlagwörter:** Cyberraum, Globalisierung, Cyber-Sicherheit, transnationale Akteure, Verschlusssachen, Cyberpower, WikiLeaks, Cyber-Policies

## V. INTRODUCCIÓN

A finales del siglo XX empezó la era de un proceso muy importante para las sociedades del mundo, este proceso es conocido como la globalización. La cual, se ha caracterizado por impulsar diferentes tipos de interacciones sociales, económicas, culturales y políticas, por medio, del uso de recursos tecnológicos los cuales que con el paso del tiempo y la innovación han desatado una revolución digital que tiene como elementos principales: a la información, nuevas tecnologías y la interconectividad, a través, del internet el que ha creado un nuevo dominio conocido como el ciberespacio, este espacio de interacción virtual ha posibilitado a que diferentes tipos de actores emerjan y puedan operar dentro del dominio guiados por sus diferentes intereses y motivaciones. Pero también, esto ha generado la preocupación sobre las amenazas del ciberespacio las cuales provienen de las diferentes acciones maliciosas empleadas para atentar contra la seguridad nacional de los Estados, o ataques cibernéticos en contra de empresas multinacionales y robo de información de individuos entre otras acciones.

Los actores que podrían causar disrupción en este dominio son diversos ya que, abarca a los Estados, grupos organizados con fines ideológicos como políticos y económicos, organizaciones de crimen organizado y por último individuos comunes con acceso a recursos tecnológicos, estos actores actúan bajo diferentes motivaciones las cuales pueden ser: actividades de inteligencia, espionaje político o industrial, robo de información o de propiedad intelectual, etc. Es por eso, que el ciberespacio proporciona el entorno físico virtual ideal en donde estas distintas motivaciones toman lugar, los impactos causados por estas amenazas tienen implicaciones sociales, económicas, y de seguridad las cuales se manifiestan en políticas nacionales como en la política exterior con repercusión a las relaciones internacionales.

La organización transnacional WikiLeaks es relevante debido a su participación internacional por medio de sus filtraciones de información confidencial sobre el gobierno estadounidense durante el 2010. Estos sucesos fueron una clara muestra sobre cómo esta apertura y expansión de la tecnología principalmente fomentada por el internet ha tenido efectos notables en la balanza de poder (Nye, 2014). Considerando lo que se ha mencionado anteriormente la presente investigación está guiada por el siguiente objetivo principal: Identificar la influencia en la formación de políticas y agencias de ciberseguridad de los Estados Unidos que fortalecieron su hegemonía en el período 2010-2015.

Partiendo de este objetivo se ha podido identificar que la participación de WikiLeaks causó un gran impacto mediático a nivel internacional, pero fue a corto plazo durante el 2010 hasta mediados del 2011. Sin embargo, esta fuga de información impulsó específicamente a que el gobierno revise en sus Agencias Federales los procesos del manejo de información confidencial y sirvió para concientizar aún más sobre las amenazas que existen en el ciberespacio por el rol de actores no estatales, también, la relación que tiene la información con el poder en la política internacional y, por lo tanto, la importancia de salvaguardarla y protegerla de actores que desean robarla y exponerla. Es por eso, que las actuaciones de WikiLeaks motivaron al gobierno de EE. UU a incrementar capacidades tecnológicas y de mayor seguridad en el ámbito de protección y manejo de información confidencial para evitar que estos incidentes vuelvan a ocurrir para que no expongan los intereses de la nación en el ámbito internacional (FISMA, 2012, p. 52).

Para centrar mejor este trabajo de investigación se planteó una hipótesis, la cual establece que la organización transnacional WikiLeaks, por medio de sus acciones anti hegemónicas en el ciberespacio, provocó la creación de políticas y agencias de

ciberseguridad que fortalecieron a la hegemonía estadounidense en el período 2010-2015. Para analizar y responder a esta hipótesis planteada, se desarrollarán tres capítulos los que están enfocados a responder a los objetivos específicos planteados.

El primer capítulo hace una descripción sobre la problemática que gira en torno a la filtración de información confidencial por parte de la organización WikiLeaks, además, se describe la respuesta del gobierno de Estados Unidos frente a estos sucesos que fueron dados durante el 2010. Con esta recapitulación de hechos se intenta identificar el tipo de repercusiones que tuvieron estas filtraciones en la política estadounidense. Para poder identificar y analizar la respuesta que dio el gobierno se encontró necesario también describir las respuestas de diferentes miembros con altos cargos dentro del gobierno de EE. UU. Por último, en el tercer apartado se cumple con el objetivo de identificar las reformas en las políticas e iniciativas más importantes sobre ciberseguridad que implementó EE. UU en los meses y años posteriores de los incidentes con WikiLeaks. En este trabajo de investigación se enfocó específicamente en identificar reformas e iniciativas que fueron creadas con el fin de aumentar y mejorar las capacidades en protección de información confidencial, acciones de respuesta, para reducir, mitigar y afrontar las amenazas que se presentan en el ciberespacio.

El segundo capítulo busca describir las reformas en las políticas e iniciativas más importantes que fueron implementadas por los principales departamentos del gobierno y presidencia, además, se hace un recorrido exploratorio para encontrar el origen de estas estrategias de ciberseguridad, lo que ayudará a identificar si la influencia de la organización WikiLeaks impulsó y provocó estos procesos durante la administración de Barack Obama. Se termina este capítulo identificando el poder blando de EE. UU al influenciar a organismos internacionales para que promuevan planes e iniciativas de ciberseguridad en el mundo ya que, la globalización ha impulsado esta naturaleza

cambiante del poder. El cual, se vuelve más complejo por los avances tecnológicos, aparición de nuevos actores en el contexto de creciente interdependencia y globalización (Keohane & Nye, 1977). Tomando en cuenta estos cambios en el sistema internacional EE. UU se vio motivado a buscar las maneras de unir fuerzas con otros países y organizaciones. Por esto, se debe resaltar que los sucesos con WikiLeaks ayudan a reafirmar que la era digital trae muchas vulnerabilidades y, por lo tanto, EE. UU necesita liderar la cooperación internacional en el ciberespacio ya que, es un lugar en el cual las amenazas crecen y mutan más rápido que las habilidades que tienen los gobiernos, es por eso que, ejercer este rol de liderazgo es esencial para incrementar su poder y seguridad dentro de este nuevo dominio.

El tercer capítulo se desarrolla con el objetivo de reconocer la relevancia de los actores transnacionales como lo es WikiLeaks el cual, por medio del uso de la información, la tecnología y el internet ha sido un ejemplo de como este tipo de actores en el ciberespacio han logrado ser factores para replantear la naturaleza del poder. En este caso se busca analizar si existe la influencia de la organización para que EE. UU se haya motivado en reforzar y aumentar sus capacidades cibernéticas las cuales dentro de este contexto también influenciaría en la perpetuación de su hegemonía y poder. Además, se realiza un análisis en el marco de la teoría de la interdependencia compleja como base y se toma el enfoque del ciberpoder que se refiere al uso de estrategias de poder duro y blando con herramientas tecnológicas (Nye, 2010).

Dentro de este capítulo se pretende analizar el cambio del juego del poder que se produce en el ciberespacio, también, se asocia el papel de la organización WikiLeaks con el uso del ciberpoder al ser una organización internacional esta crea y refleja propósitos y objetivos los cuales son transmitidos por medio de su misión la cual va a moldear el uso que va a darle al ciberpoder (Kuehl, 2009, p. 9). Esta parte de la

investigación también asocia la importancia que toma para EE. UU aumentar capacidades cibernéticas, de tal manera, con esto también aumentará su poder lo que es importante para mantener hegemonía y liderazgo dentro del ciberespacio. Por eso, en el desarrollo de este capítulo se describen las estrategias cibernéticas de EE. UU dirigidas al aumento de capacidades como el incremento del presupuesto para invertir en más capacidades cibernéticas y educación en este ámbito, y se describe el rol de las agencias federales en la implementación de la cibergobernanza para afrontar las amenazas cibernéticas, reducir la vulnerabilidad, aumentar sus capacidades y poder en el ciberespacio.

Finalmente, se realiza el capítulo del análisis en el cual se va a comprobar la hipótesis. Primeramente, se debe mencionar que la presente disertación se desarrolló con la metodología de carácter mixto, es decir, utilizando elementos de la metodología cualitativa y cuantitativa y combinándolos entre sí para apoyar los resultados de la investigación. Entonces para el desarrollo de esta parte, se describió la metodología de análisis de contenido por el autor Earl Babbie y se aplicó el método de análisis de contenido acorde al manual de investigación cualitativa de Johnny Saldaña. El método que fue empleado para analizar la muestra que se conformó por: documentos oficiales de gobierno, discursos presidenciales y de funcionarios del gobierno, informes y estrategias que se enfocan en precisar la descripción del caso y la respuesta de sus repercusiones. Por medio de la codificación de estos documentos se pudo resolver la hipótesis planteada para esta investigación.

Esta investigación a nivel académico es correspondiente al perfil de la carrera Multilingüe de Negocios y Relaciones Internacionales debido a que el tema es multidisciplinario ya que, permite explorar diferentes perspectivas desde las relaciones internacionales. Además, es un tema que busca fusionar los nuevos cambios y

elementos modernos que impulsa la globalización, los cuales, son importantes no solo para el ámbito político sino también en el social, económico y cultural. El estudio de temas sobre el ciberespacio está tomando cada vez más relevancia debido a la creciente dependencia a las tecnologías de comunicación, y también, el crecimiento económico de los países depende de las interacciones y transacciones que se hacen a través del ciberespacio, por eso, estudiar a este nuevo dominio es importante porque se encuentra en constante exploración y todos los individuos han empezado a aprender a operar dentro de él.

# 1. CAPÍTULO I: LAS REPERCUSIONES DE LAS FILTRACIONES DE WIKILEAKS EN EE. UU Y LA INFLUENCIA DE ESTAS PARA FOMENTAR INICIATIVAS, ESTRATEGIAS Y POLÍTICA DE CIBERSEGURIDAD.

En este capítulo se empezará describiendo a la organización WikiLeaks con sus antecedentes y los sucesos más relevantes protagonizados por WikiLeaks en torno a la filtración de documentos secretos que vinculen a los Estados Unidos, también se hace un recorrido por los efectos y repercusiones que estas filtraciones de información causaron a nivel nacional en EE. UU e internacional. En el segundo apartado se muestra las acciones y respuestas que realizaron los importantes miembros y jefes de departamentos del gobierno de Barack Obama y la posición oficial del gobierno frente a las actuaciones de WikiLeaks. Por último, en el tercer apartado se identifica las iniciativas más importantes que implemento EE. UU en materia de ciberseguridad para aumentar y mejorar las capacidades de respuesta, para mitigar daños provenientes de ataques cibernéticos y afrontar las amenazas que se presentan en el ciberespacio.

## 1.1 WikiLeaks y las filtraciones de información clasificada

La historia de la configuración de WikiLeaks como un actor transnacional comenzó el 04 de octubre del 2006 cuando se creó el dominio de internet wikileaks.org. Cuando se creó el dominio .org., este demuestra la intención del fundador con sus colaboradores de llevar este proyecto a una dimensión social que no era bajo intereses comerciales, lucrativos o políticos (Quian, 2016, p. 304). La idea principal de la organización se basaba en que la página web funcione como una plataforma para que las personas que deseaban participar puedan compartir documentos anónimamente. De esta manera, la organización impulsó esta metodología para compartir diferente tipo de información. Esta acción hizo que WikiLeaks se viera a sí misma como un movimiento ciudadano público que, por medio, de compartir información confidencial de interés

general estaba contribuyendo al ideal de fomentar la transparencia de los gobiernos, corporaciones, combatir la corrupción y promover la defensa de los derechos humanos entre otros (Quian, 2016, p. 304).

La organización WikiLeaks fue inspirada por el concepto de Wikipedia que es un sitio el cual permite la participación de varios usuarios para editar, crear, modificar o borrar la información que comparten, pero WikiLeaks se diferencia en que protege y resguarda el anonimato total de sus fuentes gracias al diseño altamente tecnológico de encriptación de la plataforma para que no pueda ser alterada para exponer a las fuentes o a los medios que proporcionan información, de esta manera la plataforma web quería garantizar la máxima seguridad para animar a personas a que compartan información relevante con la organización (Zifcak, 2019, p. 124).

Desde el año 2006 que la organización empezó sus operaciones con voluntarios a tiempo completo y alrededor de 1000 colaboradores en diferentes partes del mundo que trabajaban corroborando la información que el portal recibía. La organización no buscaba ser selectiva en cuanto al tipo de información que compartía, si solo era sobre gobiernos o corporaciones, sino que, buscaba lograr su objetivo de promover el ideal de una gobernanza internacional y multinacional que sea abierta, por ese motivo ningún Estado o corporación se iba a poder escapar de su mirada (Zifcak, 2019, p. 125).

La ambiciosa meta de WikiLeaks parecía imposible, pero entre el 2008 al 2010 la organización alcanzó fama internacional. Desde sus primeros años publicó miles de documentos de contenido crítico como reportes del Servicio de Investigación del Congreso de Estados Unidos, el manual de procedimientos en la prisión de Guantánamo, corrupción en Kenia, documentos de corrupción en bancos como uno en Islandia que ayudó al colapso financiero del país entre otros actos (Conde, 2014). En el año 2008 WikiLeaks da a conocer información de operaciones secretas del banco suizo

Julius Bär, que estaba por años ayudando a evadir el pago de impuestos a las grandes corporaciones, políticos y a otras personas con poder y riqueza.

El año 2010 para WikiLeaks fue el principio de su renombre a nivel internacional, el 5 de abril publicó un video con el nombre de *Collateral Murder* o en español conocido como "Asesinato Colateral", este video editado por WikiLeaks a 17 minutos muestra un ataque desde la cabina de un helicóptero Apache por parte del ejército de los Estados Unidos a diferentes ciudadanos iraquíes (Zifcak, 2019, p. 125). Lo que fue relevante del video es que cuestionaba la versión oficial del ejército estadounidense para explicar la muerte de 12 ciudadanos y dos niños gravemente heridos, que para los soldados este ataque era en respuesta a un supuesto ataque terrorista del 12 de julio del 2007 en Bagdad. Además, otro elemento que sobresale en el video es la actitud y el lenguaje despectivo de los soldados al momento de atacar a las víctimas entre las cuales se encontraban dos colaboradores de la agencia de noticias Reuters (Vega & Portillo, p. 505). Julian Assange después de la publicación expresó que la versión editada por WikiLeaks tenía el objetivo de crear el máximo impacto político (López, 2012, p. 69).

El 26 de julio del mismo año el portal publicó su primera filtración de información masiva secreta en colaboración con otros medios de comunicación de renombre: The New York Times, The Guardian, Der Spiegel en conjunto sacaron a la luz "Los diarios de guerra de Afganistán" que está compuesto por alrededor de 90 000 documentos de informes militares clasificados los cuales revelan crímenes de guerra, operaciones encubiertas, número de muertes de civiles que no se informó públicamente, técnicas de uso de tortura, violación de derechos humanos, la implicación de Pakistán en la resistencia talibán y las intenciones del ejército estadounidense por eliminar a líderes talibanes y de Al- Qaeda (Vega & Portillo, p. 505). Estos documentos que

abarcan los 6 años de combate desde el 2004 al 2010 son una muestra del poder de Estados Unidos para ocultar sus actuaciones ilegales en la guerra que han protagonizado masacres exterminando aproximadamente a unos 2 000 civiles hasta la fecha (Vega & Portillo, p. 505).

Según las perspectivas que dieron los diarios que publicaron los documentos, por ejemplo, el diario New York Times interpretó que los servicios de Inteligencia paquistaní apoyaron secretamente al movimiento talibán y por otra parte Islamabad recibía más de 1 000 millones de dólares por los Estados Unidos por ponerse en contra de los insurgentes. Por otra parte, según la interpretación del diario The Guardian llegó a concluir que los Estados Unidos tenía un grupo que trabajaba fuera de los márgenes de la ley para identificar y capturar a los líderes talibanes (Vega & Portillo, p. 506).

En octubre de 2010 se publica 91 000 informes sobre la guerra en Irak, con el nombre *Iraq War Logs o* "papeles de la guerra", estos documentos mostraron pruebas de tortura y abuso por parte del ejército estadounidense a los detenidos iraquíes. Además, el valor principal de estos informes reside en que cuenta con el registro de más de 100 000 muertes violentas que incluye a civiles durante el 2003 al 2009, estadísticas que difieren con las cifras publicadas por los Estados Unidos (Zifcak, 2019, p. 126). La revelación de estos documentos indica la guerra asimétrica que estaban enfrentando los locales con minas improvisadas frente al poderío armamentístico de los Estados Unidos (Narváez, 2012).

Para terminar el 2010 en noviembre WikiLeaks volvió a colaborar con The New York Times, The Guardian, Der Spiegel, y con dos nuevos medios de comunicación El país de España y Le Monde de Francia. Para difundir la filtración de información secreta de mayor volumen en la historia. Esta publicación denominada coloquialmente “Cablegate” es una colección de 251 287 mensajes del Departamento de Estado de

Estados Unidos con sus embajadas, consulados, misiones diplomáticas en el exterior, los cuales ponen en transparencia la política exterior estadounidense ya que, estos mensajes contienen información que revela sus mecanismos de espionaje a nivel mundial, preocupaciones geopolíticas, intereses, críticas, negociaciones entre países aliados, y otras cosas (Vega & Portillo, p. 507).

El gran valor que tiene esta filtración radica en que, por el alcance del contenido y la naturaleza de los mismos, estos cables eran la divulgación de información más controvertida. Debido, a que tenían la posibilidad de dañar la diplomacia, afectar a la maquinaria política y por supuesto repercutir en la imagen y reputación de los Estados Unidos en la comunidad internacional (Conde, 2014, p. 29). Se debe recalcar que, para los entendidos en estudios de política exterior, estos cables facilitaron el entendimiento de la cara oculta de las relaciones diplomáticas de los Estados Unidos y del desarrollo de los eventos internacionales. En otras palabras, estas revelaciones según los analistas de política exterior, las catalogan como el manual para entender la visión del mundo del país más poderoso de la actualidad ya que, por medio de esto se puede de cierta manera comprobar el poder que ejerce por medio de sus embajadas en diferentes partes del mundo para lograr sus intereses comerciales y militares (Vega & Portillo, p. 507).

### 1.1.2 Efectos Internacionales y nacionales de las filtraciones de WikiLeaks

Entre los cables que más efectos perjudiciales trajeron a los Estados Unidos fue la red de espionaje implementada a nivel global la que incluía al Secretario General de las Naciones Unidas, hasta diplomáticos y a jefes de Estado de otros países. Estos cables muestran la naturaleza de las intervenciones de EE. UU en diferentes partes del mundo ya que, estos revelaron que de cierta manera que todo lugar es parte del interés nacional de los Estados Unidos (Parmar,2014). Los cables diplomáticos causaron que

diferentes países criticaran fuertemente esta invasión a la privacidad y rechazaron el comportamiento que lo interpretaron también como una amenaza a las relaciones internacionales.

Aunque el gobierno y la opinión pública estadounidense no han mostrado más que fuertes críticas e intentos de desestabilización hacia WikiLeaks. En otras partes del mundo se pudo ver levantamientos sociales causados directamente por alguna revelación de WikiLeaks, por ejemplo, el caso de Túnez en donde los cables revelaron el desprecio de los diplomáticos estadounidenses hacia el "sistema sin control" del presidente Ben Ali y de su corrupción, todos estos cables fueron traducidos y transmitidos en sitios red locales para los tunecinos, lo que, alimentó a la radicalización de la postura molesta de la ciudadanía e incitó a que la disidencia pida la no intervención de los Estados Unidos estos sucesos terminaron con la huida del presidente Zine al-Abidine Ben Ali del país por las violentas protestas (Chrisafis, 2011). El efecto que produjo este cable puede que radique en la difusión abierta de la información para todos, lo que motivó a que los ciudadanos se unan para manifestar (Leigh & Harding, 2011).

Las manifestaciones en Túnez fueron un ejemplo de los efectos de WikiLeaks, porque motivaron a otros levantamientos populares en la región (Foreign Policy, 2011), pero estos levantamientos fueron inspirados por la información compartida por WikiLeaks que de cierta manera pueden llegar a tener efectos directos e indirectos en los cambios democráticos (Leigh & Harding,2011). El impacto de estas filtraciones se puede ver según los resultados de una encuesta del Debate de Doha realizada a principios de 2011, esta encuesta dio como resultado que en 17 países árabes países el 60% creía que las revelaciones de WikiLeaks desempeñaban un papel importante en los levantamientos en toda la región; el mismo porcentaje creía que la revelación de los

cables afectarían y cambiarían el comportamiento de los gobiernos en el futuro, lo que significaría a que gracias al trabajo de WikiLeaks el mundo se convierta en un mejor lugar (Parmar, 2014, pg.17).

Por otra parte, el impacto nacional en EE. UU por la divulgación de esta información, los trabajadores del Departamento de Estado especularon que las revelaciones pueden llegar a alterar la honestidad de las comunicaciones internas entre los diplomáticos estadounidenses alrededor del mundo con el Departamento de Estado, y producir desconfianza a las fuentes extranjeras ante la incertidumbre de que Estados Unidos no sea capaz de proteger de manera segura este tipo de información confidencial (Packer, 2010).

Sin embargo, no hay pruebas claras en las que se pueda mostrar que las revelaciones de estos cables hayan causado estos perjuicios ni tampoco existe evidencia de los daños directos en las relaciones internacionales de los Estados Unidos (Landler, 2011). Es también importante resaltar el Secretario de Defensa Robert Gates durante una rueda de prensa sobre WikiLeaks dijo que las filtraciones de información tendrían un efecto mínimo en las relaciones diplomáticas de EE. UU (Gates,2010). De igual manera, la secretaria Hillary Clinton minimizó la importancia a sus declaraciones iniciales sobre los efectos de WikiLeaks, debido a que, días después se reunió en Europa en la Organización para la Seguridad y Cooperación en donde conversó con otros líderes mundiales que le aseguraron que las relaciones diplomáticas van a mantenerse como estaban antes de la filtración de documentos por WikiLeaks (López, 2012, p. 81). Esto causó que disminuya la importancia de WikiLeaks y sus filtraciones.

## 1.2 La respuesta del gobierno de Obama a las filtraciones de WikiLeaks

En el año 2010 la organización WikiLeaks alcanzó su popularidad internacional por las diferentes revelaciones de información que vinculó o afectó directamente a los Estados Unidos. Por eso, las filtraciones de esta organización marcaron un cambio en la política nacional y exterior estadounidense, además, en la manera de controlar y proteger la seguridad nacional del país. El objetivo principal para WikiLeaks se trataba en que la difusión masiva de información tenía que lograr el mayor impacto político posible, por eso, la organización empleó la estrategia de crear mayor impacto mediático de las filtraciones trabajando con diferentes medios de comunicación reconocidos para lograr el mayor impacto político que estaban buscando.

El video "*Collateral Murder*" publicado el 5 de abril del 2010 el cual mostraba a los soldados estadounidenses abriendo fuego contra los civiles iraquíes en donde resultaron 12 muertos entre ellos 2 eran periodistas de la agencia de noticias Routers y 2 niños gravemente heridos (Conde, 2014, p.23). Este video fue la primera filtración que provocó reacciones al gobierno estadounidense que reconoció la autenticidad del video, pero el Secretario de Defensa Robert Gates expresó en defensa que el video no muestra el contexto completo de la guerra y dijo: Estas personas pueden sacar lo que quieran, y nunca se hacen responsables de ello. "No hay un antes y no hay un después" (Gates,2010). Además, dijo:

> Los soldados están en una situación hostil de combate. El video no muestra la imagen más amplia de los disparos que se estaban produciendo contra las tropas estadounidenses. Obviamente es una cosa difícil de ver. Es doloroso verlo, especialmente cuando se aprende después de lo que estaba sucediendo. Pero tú … hablaste sobre la niebla de la guerra. Estas personas estaban operando en situaciones de fracción de segundo (Gates, 2010).

En el caso de la filtración sobre los "Diarios de Guerra de Afganistán" el entonces consejero de Seguridad Nacional de EE. UU James Jones acusó a WikiLeaks en poner en peligro la vida de las personas que colaboraron en la elaboración de los informes militares y de los socios. Además, exaltó que la publicación de éstos documentos pone en vulnerabilidad y peligro la seguridad nacional del país por lo que anunció que pondrían en marcha la respectiva investigación para llegar al origen de la filtración y recalcó que los documentos publicados van desde enero 2004 a diciembre 2009, lo que abarca la mayor parte del mandato del ex presidente George W. Bush (Sánchez, 2011). Por otra parte, el portavoz del Pentágono Dave Lapan después de estudiar los documentos publicados comentó que esta filtración de información es un acto criminal, pero también reconoció que la institución al haber examinado una parte de los documentos aún no podía estimar el daño que llegaría a causar (Confidencial, 2010).

Por último, Cablegate que fue la mayor publicación de documentos gubernamentales confidenciales que logró exhibir gran parte de la diplomacia estadounidense, por lo cual despertó muchas respuestas por parte del gobierno. Para comprender de mejor manera la respuesta de la administración de Obama frente a las revelaciones de WikiLeaks, que se tornaron más agresivas después de la última gran filtración de los cables diplomáticos en diciembre del 2010. Primeramente, se debe enfocar el papel que protagonizan el Departamento de Estado, el Departamento de Defensa y del Departamento de Justicia como las ramas del Poder Ejecutivo. Por otra parte, también, es relevante el papel del congreso compuesto por el Senado y la Cámara de Representantes ya que, en conjunto son los actores que influenciaron directamente en la reacción oficial y final del gobierno hacia el accionar de WikiLeaks.

El Departamento de Estado es el encargado de manejar los asuntos de política exterior de gobierno ya que, una de sus principales responsabilidades es asesorar a la presidencia en temas internacionales, por eso, es relevante la respuesta oficial que dio la secretaria de Estado Hillary Clinton en la rueda de prensa inmediata a las filtraciones de WikiLeaks el 29 de noviembre 2010 en la que expresó la posición oficial de Washington diciendo:

> Estados Unidos condena enérgicamente la divulgación ilegal de información clasificada. Pone en peligro la vida de las personas, amenaza nuestra seguridad nacional y socava nuestros esfuerzos para trabajar con otros países para resolver problemas compartidos (…) Entonces, seamos claros: esta divulgación no es solo un ataque a los intereses de la política exterior de Estados Unidos. Es un ataque a la comunidad internacional: las alianzas y asociaciones, las conversaciones y negociaciones, que salvaguardan la seguridad global y promueven la prosperidad económica (...) Revelaciones como estas afectan el funcionamiento de un gobierno responsable. La gente de buena fe comprende la necesidad de proteger sensitivamente que las comunicaciones diplomáticas sean confidenciales para proteger el interés nacional como el interés común global (…)" (Clinton, 2010, párrafo 2)

De este discurso de Clinton se debe remarcar que comienza mostrando total desacuerdo a las actividades de WikiLeaks calificadas de "ilegales" ya que, afecta directamente en la política exterior y en la imagen de liderazgo de EE. UU al mundo en temas de combatir terrorismo, respeto y salvaguarda de derechos humanos, restablecer democracias, entre otras acciones. Con esta mención en su discurso logra enfatizar que esta agresión no solo afecta a un solo país, sino que, es un hecho que de la misma manera repercute a toda la comunidad internacional. Por lo que, este discurso suena

también como una invitación a unir fuerzas en contra de WikiLeaks ya que, su actividad pone en peligro los intereses de todos los actores estatales de la comunidad internacional.

En la segunda parte del discurso la secretaria enfatizó que están tomando "medidas agresivas" para encontrar a los responsables del robo de información, además de que ya había ordenado al Departamento de Estado y al de Defensa tomar medidas específicas para salvaguardar la seguridad y proteger la información para evitar que estos sucesos vuelvan a ocurrir. Esta parte hace referencia al tercer punto de las acciones de respuesta planteadas por el gobierno que para actuar frente a esta crisis propuso: la primera se basaba en la protección de los individuos que fueran las fuentes o colaboradores secretos de las embajadas de EE. UU; la segunda proteger los programas vigentes que sean con un fin secreto o de inteligencia; y el tercer punto era crear una política de control de daños que sea a gran escala (Conde, 2014, p.29).

Como primera medida fue pedir un reporte a todos los jefes de misión en el exterior sobre el efecto general que causarían las filtraciones en las relaciones bilaterales de cada país con EE. UU (Kennedy, 2011). Del mismo modo, se creó un "Grupo de - Trabajo WikiLeaks" compuesto por altos funcionarios del Departamento de Estado que se encargará de revisar y analizar las publicaciones de los periódicos y, además, tiene la responsabilidad de proteger los programas vigentes o personas involucradas que se encuentren en riesgo. Además, fue suspendido el acceso a la red SIPRNet NCD que es una red confidencial del Departamento de Defensa (DoD) que sirve para intercambiar información (Kennedy, 2011, p. 4). Otra acción por parte del DoD fue la creación de un equipo de mitigación para abordar los problemas de políticas, asuntos legales, seguridad, contrainteligencia y de problemas de garantía de la información por la revelación de estos documentos (Kennedy, 2011, p. 4).

Las revelaciones de WikiLeaks fueron realmente alarmantes lo que causó más presión y trabajo para el personal del gobierno. Por otra parte, el primero de diciembre tan solo 3 días después de las filtraciones la oficina de la secretaría de prensa de la Casa Blanca publicó las iniciativas del personal de seguridad nacional, iniciativas del Departamento de Estado y del Departamento de Defensa, y las iniciativas de la Oficina del Director Nacional de Inteligencia (Conde, 2014, p. 40).

En primer lugar, se anunció el nombramiento de Russell Travers como asesor principal del personal de seguridad nacional para el acceso a información y política de seguridad. El cuál iba a desempeñar principalmente la responsabilidad de identificar y desarrollar las reformas estructurales que eran necesarias por los sucesos ocasionados por WikiLeaks (The White House, 2010). Además, tiene que cumplir las tareas de brindar asesoramiento al personal de seguridad nacional enfocadas en acciones correctivas, medidas de mitigación y recomendaciones políticas, facilitar discusiones entre las agencias, desarrollar opciones con respecto a los cambios tecnológicos y de políticas para evitar la probabilidad de que puedan volver a existir fugas de información (The White House, 2010)

Se puede ver que la reacción del gobierno de Barack Obama inicialmente fue calmada, pero con las iniciativas anteriormente mencionadas es evidente que la respuesta del gobierno iba tomando mucha más intensidad, a pesar de que condenó energéticamente el accionar de WikiLeaks y estableció medidas de mitigación de daños no puso una orden judicial que restringa el acceso a esta publicación. Pero, por otra parte, también empleó una estrategia de carácter financiero y virtual para desestabilizar, censurar y parar con las actividades de WikiLeaks (Conde, 2014, p. 29).

Por consiguiente, días después de la enorme filtración de los cables diplomáticos estadounidenses la organización WikiLeaks sintió los efectos de tener a los Estados

Unidos de enemigo principal. Entre las primeras acciones que sufrió fueron ataques cibernéticos masivos por lo que WikiLeaks se vio obligado a mudar de servidor a Amazon EC2 (*elastic cloud computing*) lo que no le duró por mucho tiempo ya que, el senador Joe Lieberman impulsó una campaña de desprestigio lo que causó que Amazon elimine inmediatamente a WikiLeaks de su servidor (Conde, 2014, p. 28).

El boicot hacia WikiLeaks se intensificaba por otra parte al día siguiente de ser eliminado del servidor de Amazon, la empresa EveryDNS que es encargada de proveer servicios gratuitos de enrutamiento canceló el contrato con WikiLeaks poniendo fin a su dominio web "wikileaks.org" y a todas sus direcciones de correo electrónicas asociadas (Sánchez, 2011, p.8). A pesar de las medidas que impedían el normal funcionamiento de WikiLeaks, Julian Assange logró conseguir una dirección alterna que estaba registrada en Suiza para que el portal web no desapareciera.

Otra empresa que se sumó a aislar a WikiLeaks fue PayPal que canceló la cuenta que tenía con la organización por la cual, era imposible que reciba las donaciones para su subsistencia. La empresa argumentó que ha tomado esa decisión debido a que "el portal había violado la política de uso aceptado, la que afirma que no puede servir de cobertura para animar a otros a participar en actividades ilegales" (Conde, 2014, p. 30). De esta manera iban las empresas quitando el apoyo a WikiLeaks de la misma manera se sumó Mastercard, Visa y Post Finance que anunciaron que no procederán los pagos para WikiLeaks lo que causó gran afectación ya que, eran los métodos más rápidos y efectivos de donación en línea. La suspensión de este servicio significó la reducción sustancial de los fondos para WikiLeaks (Conde, 2014, p. 31).

A pesar de que los ataques económicos para desestabilizar a WikiLeaks estaban ya teniendo graves consecuencias a la organización, lo peor aún estaba por venir. Días después se inició la persecución en contra de Julian Assange, por lo que el Fiscal

general del Departamento de Justicia Eric Holder a principios de diciembre del 2010 durante una rueda de prensa anunció que iniciará una investigación criminal en respuesta a la filtración de información secreta (Conde, 2014, p. 32). La ex candidata a vicepresidenta Sarah Palin solicitó a Obama que emita una orden de captura contra Assange (Sánchez, 2011, p. 9). El entonces vicepresidente Joe Biden también se expresó al respecto refiriéndose a Julian Assange como un "terrorista de alta tecnología" exigió su arresto y ordenó pena de muerte (Parmar, 2014, p. 19)

Entre otros miembros de la administración de Obama el presidente del comité de seguridad nacional Peter King, le pidió al fiscal Holder y a la secretaria Clinton que empiece un juicio contra Assange bajo la Ley de Espionaje, y también, solicitó que se determine si WikiLeaks podía ser considerada como una organización terrorista extranjera[1] (Conde, 2014, p. 32). Joe Lieberman mediante su campaña de desprestigio calificó a la filtración de ser "una acción escandalosa, temeraria y despreciable, que pondrá en peligro la capacidad de EE. UU y sus socios de defender sus intereses" y pidió a Obama utilizar todas las herramientas legales necesarias para terminar con todas las actividades de WikiLeaks antes de que haya más perjuicios.

### 1.2.1 Percepciones de la opinión pública estadounidense sobre las filtraciones de WikiLeaks

No solo la administración de Obama estaba expresando su posición de rechazo a las actividades de WikiLeaks, sino también la opinión pública apoyaba el discurso y la

[1] A partir de las filtraciones del 2010 el departamento de justicia de EE. UU abrió una investigación criminal con el objetivo de presentar un caso contra Assange por las publicaciones de WikiLeaks. Actualmente el Sr. Assange enfrenta cadena perpetua por múltiples cargos que incluyen conspiración, robo y espionaje electrónico, un delito de terrorismo. El director de la CIA, Mike Pompeo (ahora secretario de Estado) Ha declarado que Julian Assange "no tiene derechos de la Primera Enmienda" y ha descrito a WikiLeaks como una "agencia de inteligencia hostil no estatal". Por lo tanto, la CIA está trabajando para "derribar" a WikiLeaks (Justice for Assange, 2020)
Ver ¿Por qué el gobierno de Estados Unidos quiere enjuiciar a Julian Assange? Justice for Assange recuperado de: https://justice4assange.com/

posición del gobierno. La mayor parte de la población estadounidense según encuestas de diferentes medios de comunicación como The Washington Post, CBS News y CNN los resultados arrojaron que la mayoría de los ciudadanos encuestados estaban de acuerdo con que el incidente iba a causar daños en las relaciones internacionales de los Estados Unidos.

En la encuesta que realizó *Opinion Research Corporation* a 1 008 adultos del 17 al 19 de diciembre del 2010 con la pregunta si "se aprobaba o se desaprobaba la información que WikiLeaks publicó en su sitio web" los resultados mostraron que el 77% estaba en desacuerdo, el 20% aprobaba y solo el 3% no dio opinión. Por otra parte, la encuesta de CBS News realizada a 1 067 adultos entre el 29 de noviembre al 2 de diciembre 2010 planteó una pregunta interesante sobre "si el público debe tener el derecho a saber todo lo que hace el gobierno" solo el 25% estuvo de acuerdo de que se debe saber toda la información, el 73% dijo que no se debe tener el derecho a saber los secretos del Estado para salvaguardar la seguridad y el 2% dijo que no sabía.

En la encuesta de The Washington Post con una muestra de 1 001 adultos realizada del 9 al 12 de diciembre. Se encontró interesante que cerca del 59% dijo que el gobierno debe arrestar a Julian Assange. Los resultados de las encuestas son claras la mayoría de los ciudadanos estadounidenses tiene la percepción de que WikiLeaks pone en riesgo la seguridad nacional y perjudica las relaciones internacionales de los Estados Unidos, esta posición pública es evidentemente agresiva, pero es importante resaltar como las reacciones anteriormente mencionadas han influido de cierta manera en la opinión pública que es la que refleja los esfuerzos que pusieron el gobierno, medios de comunicación, y principales corporaciones para desviar la atención en el contenido de las publicaciones de WikiLeaks y de cierta manera destruir la credibilidad de la misma (Gosztola, 2011).

## 1.3 Incremento de las capacidades cibernéticas y fomento de las iniciativas de ciberseguridad en EE. UU

Desde la llegada de Barack Obama a la presidencia se identificó que entre los retos que los Estados Unidos afrontará se encuentra la protección del ciberespacio, por eso, en el año 2009 ordenó al Consejo de Seguridad Nacional y al Consejo del Departamento de Estado que se realice una Revisión de la Política del Ciberespacio de 60 días que incluía a los planes y programas de todo el gobierno federal. Esta Revisión de la Política del Ciberespacio identificó deficiencias en políticas y estructuras legales que se tradujeron en grandes vulnerabilidades para la seguridad cibernética del país. También, concluyó que es importante incrementar el papel de liderazgo del gobierno, aumentando la responsabilidad en el ciberespacio, por lo cual se encontró necesario crear el cargo de coordinador de seguridad cibernética con acceso al presidente (CCDCOE, 2016).

Entre otras cosas, sugirió que se fomente la colaboración entre el poder ejecutivo y diferentes actores claves en la ciberseguridad de EE. UU como gobiernos estatales, locales y con el sector privado para asegurar la prevención de futuros incidentes en el ciberespacio (CCDCOE, 2016). Además, se considera necesario invertir en la investigación, innovación, y desarrollo de destrezas para afrontar los desafíos digítales actuales. Estas actividades mencionadas anteriormente son el resultado de la revisión de la política del ciberespacio.

A raíz de los resultados de la revisión de la política del ciberespacio, el presidente Barack Obama por medio de la oficina ejecutiva de la presidencia publicó en el 2010 la nueva “La Iniciativa Global sobre Ciberseguridad Nacional” o (*The Comprehensive National Cybersecurity Initiative*) con sus siglas CNCI en inglés. En la cual determinó que las actividades propuestas por el CNCI desempeñan una función

principal para lograr cumplir con las recomendaciones de la revisión de la política del ciberespacio ya que, las recomendaciones mencionadas anteriormente son parte también de esta iniciativa (CNCI,2010). Esta iniciativa resalta que la administración de Obama ha identificado a la ciberseguridad como uno de los desafíos más serios tanto en el ámbito económico y de seguridad nacional para el país (CNCI, 2010)

Las iniciativas del CNCI se convirtieron en un elemento clave de la estrategia de seguridad cibernética de EE. UU en la administración de Obama ya que, estas fueron elaboradas con el fin de apoyar directamente al logro de las recomendaciones que surgieron de la Revisión de la Política del Ciberespacio del 2009. Por lo que, mediante este documento se desarrolló doce iniciativas para asegurar a los EE. UU en el ciberespacio, pero estas iniciativas se formularon en base a tres objetivos principales para alcanzar la seguridad los cuales son:

1. Establecer una primera línea de defensa contra las amenazas inmediatas de hoy: este objetivo quiere mejorar las capacidades de acción rápida con el fin de reducir las vulnerabilidades.
2. Defenderse de todo el espectro de amenazas: lo cual lo piensa conseguir mejorando las capacidades de contrainteligencia y aumentando la seguridad de la cadena de suministros de tecnologías de información clave.
3. Extender el futuro del entorno de la ciberseguridad: para lo que se propone ampliar la educación cibernética, trabajar en desarrollar estrategias que puedan disuadir y reducir las actividades maliciosas en el ciberespacio.

En base a estos tres objetivos se desarrolló las 12 iniciativas del CNCI que tiene la función de fortalecer capacidades fundamentales para que los objetivos puedan ser cumplidos. Estas iniciativas están detalladas a continuación:

*Tabla 1.1 The Comprehensive National Cybersecurity Initiative 2010*

| Tabla de las 12 Iniciativas que componen la *Comprehensive National Cybersecurity Initiative* del 2010 |
|---|

| | |
|---|---|
| 1. Administrar la Red de los gobiernos federales como una sola red con conexiones de Internet confiables | 2. Implementar un sistema de detección de intrusos con sensores en todo el gobierno federal |
| 3. Fomentar el despliegue de sistemas de prevención de intrusiones en todo el gobierno federal | 4. Coordinar y redirigir los esfuerzos de investigación y desarrollo (I&D) |
| 5. Conectar los centros actuales de operaciones cibernéticas para mejorar la conciencia situacional | 6. Desarrollar e implementar un plan de contrainteligencia cibernética (CI) en todo el gobierno |
| 7. Aumentar la seguridad de las redes clasificadas | 8. Expandir cibereducación |
| 9. Definir y desarrollar programas y estrategias perdurables de tecnología | 10. Definir y desarrollar estrategias y programas duraderos de disuasión |
| 11. Desarrollar un enfoque múltiple para la gestión y manejo de riesgos a nivel global | 12. Definir el rol del gobierno federal para extender la ciberseguridad en dominios de infraestructura crítica |

Fuente: Comprehensive National Cybersecurity Initiative, 2010
Elaborado por: Torres, P. 2020

La Iniciativa Global sobre Ciberseguridad Nacional (CNCI) con sus doce iniciativas mencionadas anteriormente, no fueron las únicas acciones planteadas por el presidente Obama en materia de ciberseguridad. Durante su administración la preocupación que generaron las publicaciones de WikiLeaks fueron un incentivo más para calificar de prioridad nacional a la ciberseguridad. En cuanto a las iniciativas impulsadas por la presidencia se empezó designando al nuevo coordinador de Ciberseguridad, poco después Obama presentó su primera Estrategia de Seguridad Nacional en mayo del 2010, la cual fue la primera estrategia que le dedicó especial atención a las “amenazas cibernéticas” (Vergara & Trama, 2017).

Este documento manifestó: "Las capacidades espaciales y ciberespaciales que alimentan nuestra vida cotidiana y las operaciones militares son vulnerables a la interrupción y al ataque” (Vergara & Trama, 2017). Además, a lo largo de la estrategia aparece 24 veces la palabra “Cyber” y el terminó “espacio cibernético” aparece por primera vez con la caracterización de ser una de las más graves amenazas a la seguridad

nacional (Vergara & Trama, 2017). Lo cual, es una muestra evidente sobre cómo impactaron las filtraciones en el incremento de la importancia de la ciberseguridad.

Entre las políticas identificadas creadas por la Política de la Directiva Presidencial fue la siguiente: Preparación Nacional (PPD-8) creada con el fin de fortalecer la seguridad y la resistencia de los Estados Unidos ante amenazas que representan el mayor riesgo para la seguridad nacional entre estos riesgos están los ciberataques, actos terroristas, y catástrofes naturales. También, entre las iniciativas presidenciales en noviembre del 2010 firmó la Orden Ejecutiva 13556 sobre el control de información no clasificada, para gestionar la información que necesita tener mayor protección. En octubre del 2011, después de que la Administración completó una revisión exhaustiva a las agencias federales por los incidentes protagonizados por WikiLeaks. Esta revisión estaba dirigida con el fin de revisar las capacidades de protección de información clasificada del gobierno ante las amenazas internas y ataques externos, como resultado de esta revisión el Presidente Obama firmó la Orden Ejecutiva 13587 sobre "Reformas estructurales para mejorar la seguridad de las redes clasificadas y el intercambio responsable y la salvaguarda de la información clasificada" (FISMA, 2012, p. 52).

Por otra parte, el Departamento de Seguridad Nacional (*Department of Homeland Security DHS*) tiene tareas importantes ya que, es el principal departamento que está encargado de asegurar y proteger a la nación de todas las amenazas, es por eso, que es importante identificar las iniciativas impulsadas y desarrolladas que son más importantes para tratar el tema de ciberseguridad. Entre las primeras iniciativas está el "Plan Nacional de Respuesta a los Incidentes Cibernéticos" (NCIRP) publicado en septiembre del 2010 este plan también emerge de las iniciativas planteadas por el CNCI

y también de la Revisión de la Política del Ciberespacio para establecer las estrategias sobre como la nación va a responder ante incidentes cibernéticos cotidianos y graves.

El DHS también realizó la Revisión Cuadrienal de Seguridad Nacional (QHSR) del 2010 y entre sus misiones para ese año se propuso Salvaguardar y Asegurar el ciberespacio ya que, es necesario que los Estados Unidos esté preparado para afrontar amenazas cibernéticas a corto y a largo plazo. Esta revisión fue la que impulsó a que se elabore *Blueprint for a Secure Cyber Future* este es el plan Para un Futuro Cibernético Seguro especialmente diseñado para proporcionar acciones enfocadas en dos áreas: protección de la infraestructura de información crítica y el fortalecimiento del ecosistema cibernético, las cuales son importantes para implementar con éxito la Estrategia de Seguridad Nacional y lograr la misión establecida por Revisión Cuadrienal de Seguridad Nacional (CCDCOE, 2016, p. 8).

Además, por el liderazgo de los Estados Unidos en la política mundial y por la necesidad de unir fuerzas para operar con seguridad en el ciberespacio, también incremento iniciativas a nivel internacional en mayo del 2011 presentó la "Estrategia Internacional para el Ciberespacio, Prosperidad, seguridad y apertura en un mundo de red", este documento plantea la misión que tiene los EE. UU con la comunidad internacional para actuar sobre los riesgos que tiene el ciberespacio para todas las naciones. En julio del 2011 el Departamento de Defensa *(Department of Defense DoD)* publicó su Estrategia para Operar en el Ciberespacio con alcance internacional para minimizar el impacto de los ataques cibernéticos ya que, dentro de las iniciativas estratégicas del plan hace hincapié en construir relaciones sólidas con aliados de EE. UU y otros socios internacionales para fomentar y fortalecer la ciberseguridad colectiva.

En julio del 2011 el DHS publicó "La Estrategia Presidencial para Combatir el Crimen Organizado Transnacional" esta estrategia también tiene alcance global debido

a que la lucha contra el crimen transnacional no puede ser un objetivo individual. EE. UU menciona que dentro del crimen transnacional el cibercrimen está involucrado dentro de las principales amenazas para los Estados. Por lo tanto, esta estrategia busca fomentar la cooperación internacional para fomentar tecnologías y compartir inteligencia para acabar con el cibercrimen y las otras amenazas del crimen transnacional.

Las filtraciones de WikiLeaks especialmente las del 2010 marcaron de cierta manera la política nacional y exterior de los Estados Unidos. Aunque las revelaciones causaron impacto a corto plazo durante finales del 2010 y a principios del 2011, estos acontecimientos sirvieron para que el gobierno de Barack Obama preste más atención a las amenazas cibernéticas como ningún otro gobierno lo había hecho antes. Debido a que, gracias a la participación de WikiLeaks se evidenció las fallas y los errores en la seguridad de los EE. UU (FISMA, 2012, p. 52). Por otra parte, la postura estadounidense fue que la organización era una amenaza a la seguridad nacional.

Sin embargo, no se han encontrado pruebas contundentes que puedan mostrar los daños causados a la seguridad nacional, pero, lo que si se ha podido evidenciar son las diferentes y numerosas iniciativas impulsadas por EE. UU para mejorar sus capacidades cibernéticas para evitar que estos sucesos vuelvan a ocurrir ya que, los EE. UU es uno de los países pionero en desarrollar iniciativas tecnológicas para el ciberespacio y su objetivo es mantenerse en la posición de liderar dentro y fuera de él. En este capítulo se logró identificar los planes, estrategias, políticas y reformas más relevantes a lo que compete a reforzar la ciberseguridad y las acciones de respuesta después de las filtraciones de WikiLeaks. Estas iniciativas identificadas en este capítulo serán descritas en el siguiente para mejorar el entendimiento de la ciberseguridad estadounidense.

## 2. CAPÍTULO II: EL CIBERESPACIO: COMO UN NUEVO ESCENARIO PARA EL SURGIMIENTO DE AMENAZAS A LA SEGURIDAD NACIONAL

En este capítulo se describirán las iniciativas impulsadas por el gobierno de Barack Obama y de la Organización de las Naciones Unidas (ONU) como organización representante de la comunidad internacional, a raíz de la necesidad creciente de enfrentar a los desafíos e incidentes que se pueden ocasionar en el ciberespacio por la presencia de actores transnacionales maliciosos y la creciente oportunidad de fomentar amenazas cibernéticas por la innovación tecnológica. Para explicar mejor estas iniciativas a lo largo de este capítulo se podrán ver las estrategias o planes de ciberseguridad más relevantes primeramente las establecidas por la oficina presidencial de los Estados Unidos, en el segundo apartado se describirán las iniciativas impulsadas por el Departamento de Seguridad Nacional (DHS) el principal departamento con la tarea de liderar iniciativas de ciberseguridad para asegurar y proteger a la nación de amenazas. Por último, el tercer apartado trata del papel y responsabilidad de los Estados Unidos y de las Naciones Unidas para apoyar iniciativas para actuar en el ciberespacio incentivando a la cooperación internacional de diferentes actores gubernamentales y no gubernamentales en la ciberseguridad.

### 2.1 La presidencia de Barack Obama y sus esfuerzos para reducir las amenazas y riesgos del ciberespacio que afectan a la seguridad nacional.

El presidente Barack Obama desde su campaña presidencial se enfocó en aumentar las capacidades cibernéticas, a lo que señaló en sus discursos que entre las amenazas principales del siglo 21 constan las cibernéticas. Además, hizo hincapié que todos los ciudadanos dependen de manera directa e indirecta de los sistemas de redes de información, por lo que resaltó su importancia ya que, estos son fundamentales para la prosperidad económica, para la buena marcha de las infraestructuras críticas y la

seguridad nacional. Por eso, estos sistemas se vuelven elementos vulnerables para ataques terroristas (Pastor, Pérez, Arnáiz de la Torre, & Toboso, 2009). Entre otras promesas que hizo el mandatario en materia de ciberseguridad fueron; declarar a las ciberinfraestucturas como un activo estratégico y también propuso nombrar un asesor nacional de ciberseguridad.

La nueva administración de Obama, estaba consciente de los desafíos en materia de ciberseguridad que iba a afrontar en los siguientes años. Por eso, empezó calificando de "prioridad nacional" a la ciberseguridad de los sistemas de Estados Unidos. Ante el peligro de asaltos latentes a las redes informáticas, estos provocan afectaciones de tipo económico y militar que gravemente tiene que enfrentar EE.UU. Por lo tanto, anunció que se va a desarrollar planes, políticas y estrategias para alcanzar máxima seguridad y protección a las redes; y si es necesario Estados Unidos estaría preparado para iniciar una nueva guerra que será desarrollada en el ciberespacio (Pastor, Pérez, Arnáiz de la Torre, & Toboso, 2009, pág. 74).

En cuanto a la creación del puesto de coordinador de Ciberseguridad el 22 de diciembre del 2009 se designó a Howard Schmidt[2] que fue asesor de ciberseguridad de la administración de George W. Bush. Por sus cuarenta años de experiencia en el gobierno, en asuntos de negocios, legales, policiales y políticos. Él fue el candidato ideal para asumir la responsabilidad de coordinar y sincronizar las políticas de administración y asistir al Presidente en temas de seguridad en el espacio cibernético (Vergara & Trama, 2017). En su discurso como nuevo coordinador manifestó sobre la importancia de incrementar la seguridad en la red diciendo: "En nuestro mundo digital

2 Ver President Obama & White House Cyber Security Chief Howard Schmidt. Recuperado de: https://obamawhitehouse.archives.gov/photos-and-video/photos/president-obama-white-house-cyber-security-chief-howard-schmidt

las tecnologías de información que dependemos todos los días se nos presentan como una gran oportunidad y a su vez como un gran peligro para nuestra seguridad nacional, seguridad pública y nuestra competitividad económica"[3] (Schmidt, 2009).

Los Estados Unidos se ha caracterizado por ser pionero en la formulación de políticas de seguridad cibernética a nivel nacional desde 1988 con la creación del primer Equipo de Respuesta de Emergencia Cibernética conocido actualmente como el US-CERT (Schackelford & Craig, 2014). Sin embargo, el gobierno de Obama se ha destacado por estar activamente implementando iniciativas y estrategias para crear una integrada política de ciberseguridad ya que, esta administración es consciente de que los desafíos son menos convencionales y son de carácter transnacional lo que significó que era necesario y urgente incrementar capacidades, para de tal manera integrar efectivamente el poder de los Estados Unidos (Villalba, 2015, p. 131).

El presidente Obama lanzó su primera Estrategia de Seguridad Nacional en mayo del 2010, la cual, es donde se plasma la visión sobre la situación mundial, amenazas, oportunidades que va a afrontar la nación en los siguientes años, también, este documento aporta con los lineamientos establecidos para abordar estos temas y garantizar la seguridad de los Estados Unidos (Ministerio Español de Defensa, 2010). Como se mencionó en el anterior capítulo esta estrategia remarca atención especial a las amenazas cibernéticas y reconoce que los ataques cibernéticos no solo son protagonizados por grupos terroristas, sino que Obama también reconoció: "Las amenazas que enfrentamos varían desde hackers criminales individuales hasta grupos criminales organizados, desde redes terroristas hasta naciones avanzadas" (NSS, 2010).

[3] Ver discurso Howard Schmidt en: https://obamawhitehouse.archives.gov/photos-and-video/video/a-commitment-cybersecurity

La estrategia destaca la importancia que ha tenido la globalización a lo largo de los años en ser parte del progreso de las sociedades, pero también, ha sido la causante de generar nuevas amenazas como la difusión de tecnologías peligrosas, terrorismo internacional, aceleración del cambio climático, fomentar crisis económicas, proliferación de armas nucleares entre otras más. Factores que han motivado a que los EE. UU deban tomar la iniciativa de incentivar acciones colectivas y la cooperación ya que, es imposible que puedan responder solos a los retos globales (Ministerio Español de Defensa, 2010).

La estrategia del 2010 señala al ciberespacio como una nueva amenaza a diferencia de las otras estrategias anteriores como la del 2002 en la que no se desarrolló este concepto y la del 2006 que solo lo mencionó como un riesgo disruptivo junto a la biotecnología (Ministerio Español de Defensa, 2010). Por el contrario, para la administración de Obama el ciberespacio se vuelve un concepto clave de seguridad ya que, es considerado que en el ciberespacio surgen amenazas que representan uno de los desafíos más serios que enfrenta el mundo en la actualidad (NSS, 2010). Por medio de esta se muestra que el gobierno de EE. UU está consciente de que cada día crece la dependencia a las redes de información y de igual manera se incrementan los enemigos en el ciberespacio que buscan atacar a estas redes del Estado. Por eso, es importante la acción de declarar a la infraestructura digital como un activo estratégico nacional y su protección es una prioridad en esta estrategia (Ministerio Español de Defensa, 2010).

La NSS plantea dos puntos fundamentales para disuadir, prevenir, detectar, defender y recuperarse rápidamente de las intrusiones y ataques cibernéticos por medio de la inversión en personas y tecnología, lo que significa que trabajarán con el gobierno y el sector privado para diseñar tecnologías más seguras que brinden más capacidad de protección, fomentar la investigación y el desarrollo para lograr la innovación necesaria

para enfrentar los retos y promover campañas a nivel nacional sobre concientización en temas de ciberseguridad y alfabetización digital (NSS, 2010). El segundo punto es el Fortalecimiento de las asociaciones, lo que quiere decir que ampliaron las formas de trabajo fortaleciendo e incrementando alianzas internacionales para trabajar en el desarrollo de normas para una conducta aceptable en el ciberespacio; implementar leyes relativas al delito cibernético; preservación de datos, protección y privacidad; y enfoques para la defensa de la red y la respuesta a los ciberataques (NSS, 2010).

Entre otras respuestas de la administración de Obama referente a los incidentes de ciberseguridad el 30 de marzo del 2011 se impulsó la Política de la Directiva Presidencial (PPD-8): Preparación Nacional con el objetivo de fortalecer la seguridad y la resistencia de los Estados Unidos ante amenazas que son de alto riesgo a la seguridad nacional entre estos riesgos están los ciberataques, actos terroristas, y catástrofes naturales (PPD-8, 2011). Con esta política se buscó impulsar la acción del Gobierno Federal y aumentar su preparación integral por medio de la implementación de un sistema nacional de resiliencia que le permita a los EE. UU construir y mejorar las capacidades necesarias para prevención, protección. mitigación, recuperación y respuesta ante las amenazas (PPD-8, 2011).

Para lograr cumplir con el objetivo de esta política (PPD-8) es fundamental estar informado con los detalles específicos del riesgo de amenazas y vulnerabilidades ya que, con estos detalles se elaborará un plan operativo interinstitucional que incluirá conceptos más detallados para las diferentes operaciones para la efectiva integración de recursos y personal (PPD-8, 2011). El secretario de Seguridad Nacional es el responsable de coordinar conjuntamente con los gobiernos estatales, sector privado, organizaciones no gubernamentales entre otros actores las acciones internas de preparación para todos los peligros de todos los departamentos y agencias (PPD-8,

2011). Esta política de respuesta firmada por el presidente Obama muestra que impulsó que la preparación sea una responsabilidad compartida.

El presidente Obama en 2011 también firmó la Orden Ejecutiva 13587 – "Reformas estructurales para mejorar la seguridad de las redes clasificadas, el intercambio responsable y la salvaguarda de la información clasificada". Orden presidencial que fue impulsada por las amenazas y ataques cibernéticos que ha recibido los EE. UU en los últimos meses, los que han animado la iniciativa de aumentar la protección y la salvaguarda de información clasificada por medio de establecer expectativas comunes, institucionalización de mejores prácticas del poder ejecutivo; y permitiendo una implementación y participación flexible en toda la rama ejecutiva (Executive Order 13587, 2011)

Esta orden está dividida en seis secciones que son detalladas a continuación:

*Tabla 2.1 Orden ejecutiva 13587 "Reformas estructurales para mejorar la seguridad de las redes clasificadas, intercambio responsable y la salvaguarda de la información clasificada"*

| **Orden ejecutiva 13587 – "Reformas estructurales para mejorar la seguridad de las redes clasificadas, intercambio responsable y la salvaguarda de la información clasificada"** | |
|---|---|
| Sección 1. Política | Aplicar reformas estructurales para garantizar el intercambio responsable y la protección de la información clasificada en las redes informáticas |
| Sección 2. Responsabilidades generales de las Agencias | Los dirigentes de las agencias tienen la responsabilidad de designar un senior oficial que supervise el proceso de compartir información clasificada y los esfuerzos de la agencia.<br>Implementar un programa de detección y prevención de amenazas internas |
| Sección 3. Comité Directivo de Intercambio de Información y Protección | Los miembros del comité deben ser funcionarios de los Estados Unidos designados por los jefes de diferentes departamentos de Estado.<br><br>El deber principal de este comité es garantizar la rendición de cuentas de alto |

| | |
|---|---|
| | nivel para el desarrollo coordinado entre agencias y la implementación de políticas sobre el intercambio y protección de información clasificada en redes informáticas. |
| Sección 4. Oficina de intercambio y protección de información clasificada. | Brindar asesoramiento para la Protección de la Información Clasificada en Redes de Computadores y también al Grupo de trabajo sobre amenazas internas en el desarrollo de un programa efectivo para monitorear el cumplimiento de las políticas y estándares establecidos.<br><br>Consultar con los Departamentos para garantizar la coherencia con las políticas y normas bajo la Orden Ejecutiva 13526 del 2009 |
| Sección 5. Agente ejecutivo para salvaguardar la información clasificada en redes de computadoras. | El Secretario de Defensa y el Director de la Agencia de Seguridad Nacional actuarán conjuntamente como el Agente Ejecutivo.<br><br>Responsabilidades:<br>Desarrollar políticas y estándares efectivos de salvaguarda técnica en coordinación con el Comité de Sistemas de Seguridad Nacional CNSS<br><br>Informes anuales al Comité Directivo anualmente sobre el trabajo del CNSS, incluidas las recomendaciones para mejorar la eficacia<br><br>Realizar evaluaciones del cumplimiento de la agencia con las políticas y estándares de protección establecidos. |
| Sección 6. Grupo de trabajo sobre amenazas internas. | Desarrollar un programa a nivel gubernamental (programa de amenazas internas) para disuadir, detectar y mitigar las amenazas internas.<br><br>Proporcionar un análisis de los nuevos y continuos desafíos de amenazas internas que enfrenta el Gobierno de los Estados Unidos. |

Fuente: The White House Office of the Press Secretary, 2011
Elaborado por: Torres, P. 2020

## 2.2 Iniciativas impulsadas por el Departamento de Seguridad Nacional (DHS)

El Departamento de Seguridad Nacional con sus siglas en inglés DHS es el principal departamento que tiene la misión vital de asegurar y proteger a la nación de

todas las amenazas existentes, lo que incluye a la ciberseguridad como una de las acciones principales para proteger la seguridad nacional de los EE. UU, por eso, se va a describir las iniciativas que impulsó este departamento para actuar en el ciberespacio, contrarrestar ataques y minimizar los riesgos. El secretario de seguridad nacional es responsable de gestionar y coordinar las respuestas ante ciberincidentes significativos. Su principal tarea consiste en coordinar e integrar información de los centros federales de seguridad cibernética; gobiernos estatales, locales y del sector privado (NCIRP, 2010).

El Departamento de Seguridad Nacional (DHS) respondió a los incidentes de ciberseguridad con el "Plan Nacional de Respuesta a los Incidentes Cibernéticos" con sus siglas en inglés (NCIRP) en septiembre del 2010. Este plan es el resultado de la Iniciativa Global Sobre Ciberseguridad Nacional (CNCI) y de la Revisión de la Política del Ciberespacio, este plan establece la dirección estratégica de como los EE. UU responderá a los incidentes cibernéticos y como estas acciones se transforman en respuestas coordinadas a nivel nacional. Además, hace referencia que estas iniciativas iban a mejorar la seguridad cibernética nacional y fortalecer la defensa para que se vuelva mucho más sólida (NCIRP, 2010).

Los objetivos principales que se establecieron en el NCIRP fueron: mejorar las respuestas y garantizar que las políticas federales de respuesta a incidentes cibernéticos faciliten la rápida coordinación nacional necesaria para actuar en defensa durante incidentes cibernéticos. Es un plan muy prometedor ya que, vincula varias políticas e iniciativas en un solo plan que también está diseñado para coordinar en conjunto entre gobiernos federales, estatales, locales, el sector privado y socios internacionales principalmente en la construcción de mecanismos necesarios y efectivos para responder a un incidente y a la recuperación del mismo a corto plazo (NCIRP,2011, p. 10).

El NCIRP establece los lineamientos estratégicos de como la nación debe responder a incidentes cibernéticos cotidianos, es decir, este plan se enfoca específicamente en construir mecanismos necesarios para responder a estos incidentes cibernéticos significativos, con esto se refiere a que es un conjunto de condiciones en el ciberespacio que requiere mayor esfuerzo y coordinación nacional (NCIRP,2011).

Entre otras iniciativas del DHS se encuentra la Revisión Cuadrienal de Seguridad Nacional de febrero del 2010 (QHSR) entre sus misiones propuso Salvaguardar y Asegurar el ciberespacio, debido a que en los últimos años las transacciones económicas y sociales se han mudado al ciberespacio, lo que representa un riesgo latente ya que, diferentes actores se empoderan para realizar diferentes tipos de robos o causar grandes daños. Es por esto, que el QHSR quiere un ciberespacio que respalde una infraestructura segura en donde se pueda promover con confianza los intereses económicos y mantener la seguridad nacional (QHSR, 2010).

Para lograr esta misión el QHSR propuso metas para lograr que EE. UU esté preparado para afrontar amenazas cibernéticas y los desafíos del futuro del ciberespacio. Estas metas están compuestas por objetivos que se pueden ver en la siguiente tabla:

*Tabla 2.2 Metas y objetivos para el ciberespacio en la Revisión Cuadrienal de Seguridad Nacional*

| **Salvaguardar y Asegurar el Ciberespacio<br>Metas y Objetivos** |
|---|
| Meta 1. Crear un entorno cibernético seguro y resistente<br><br>Objetivos:<br><br>• Entender y priorizar las amenazas cibernéticas: identificar y evaluar las amenazas más peligrosas no solo para las redes federales sino también para el sector privado e individuos.<br>• Administrar riesgos para el ciberespacio: proteger y crear sistemas de información resistentes y confidenciales |

| |
|---|
| • Prevenir el delito cibernético y otros usos maliciosos del ciberespacio: interrumpir las organizaciones criminales y otros actores maliciosos involucrados en delitos cibernéticos.<br>• Desarrollar una sólida capacidad de respuesta a incidentes cibernéticos público-privados: administrar los incidentes cibernéticos desde la identificación hasta la resolución de una manera rápida y replicable con una acción rápida y apropiada. |
| Meta 2. Promover el conocimiento y la innovación en ciberseguridad<br><br>Objetivos:<br><br>• Mejorar la conciencia pública: garantizar que los individuos reconozcan los desafíos de seguridad cibernética y tengan conocimiento para abordarlos<br>• Fomentar una fuerza laboral dinámica: desarrollar la base del conocimiento nacional y aumentar las capacidades de capital humano para tener éxito contra las amenazas actuales y futuras.<br>• Invertir en tecnologías, técnicas y procedimientos innovadores: crear y mejorar la ciencia, la tecnología, los mecanismos de gobernanza y otros elementos necesarios para mantener un entorno cibernético seguro y resistente. |

Fuente: Department of Homeland Security (QHSR), 2010
Elaborado por: Torres, P. 2020

A raíz de la Revisión Cuadrienal de Seguridad Nacional (QHSR) el Departamento de Seguridad Nacional (DHS) estableció *Blueprint for a Secure Cyber Future*, que es una estrategia que tiene el fin de ser un plan claro de acción en el ámbito de la ciberseguridad y que también logra implementar elementos de la Estrategia de Seguridad Nacional del 2010. Este plan también busca reflejar la importancia del ciberespacio para la economía, seguridad y estilo de vida de los Estados Unidos (BSCF, 2011). Cuando se presentó este *Blueprint for a Secure Cyber Future* la secretaria del DHS Janet Napolitano en su mensaje escrito en la presentación de este documento dijo, que esta estrategia está diseñada especialmente para proteger los sistemas y activos críticos que son de vital importancia para los Estados Unidos y fomentar a que las

tecnologías de información con el tiempo se vuelvan más fuertes y resistentes para que el gobierno y los individuos gocen de más seguridad en el ciberespacio (BSCF, 2011).

La estrategia destaca que en el ciberespacio se encuentran diferentes tipos de amenazas desde piratas informáticos, grupos delictivos organizados hasta Estados-Nación tecnológicamente avanzados, los cuales, son capaces de afectar la competitividad económica y la seguridad nacional del país, por el robo de propiedad intelectual, datos financieros, información personal y documentos gubernamentales secretos entre otras acciones de alto riesgo. Además, este plan contempla el trabajo en conjunto de varios departamentos y agencias federales para crear este plan y garantizar la coherencia con otras iniciativas en común como lo es La Estrategia de Seguridad Nacional, la Estrategia del Departamento de Defensa para Operar en el Ciberespacio, la Estrategia del Presidente para Combatir la Delincuencia Organizada Transnacional y la Estrategia Internacional para el Ciberespacio (BSCF, 2011).

El plan está elaborado con dos objetivos principales el primero es "proteger la infraestructura de información crítica actual" que se enfoca en los sistemas y activos dentro del ecosistema cibernético que son de gran importancia para los Estados Unidos y el segundo es "construir un ecosistema cibernético"[4] más fuerte para el mañana este se enfoca principalmente en impulsar cambios en la forma en que los individuos y los dispositivos trabajan juntos para lograr más seguridad en el ciberespacio (BSCF, 2011).

En el siguiente cuadro se pueden ver las acciones para cumplir con estos dos objetivos:

[4] El ecosistema cibernético: es global e incluye infraestructura de información del gobierno y del sector privado; la variedad de personas que interactúan, procesos, tecnologías de información y comunicación, y las condiciones que influyen en su seguridad cibernética (BSCF, 2011, p. 43).

*Tabla 2.3 Acciones para cumplir con los objetivos de la iniciativa Blueprint for a Secure Cyber Future*

| **Áreas principales de acción:** | ***Proteger la Infraestructura de información critica*** | ***Construir un ecosistema cibernético más fuerte para el mañana*** |
|---|---|---|
| Acciones para lograr los dos objetivos propuestos: | 1. Reducir la exposición al riesgo cibernético<br>2. Garantizar la respuesta prioritaria y la recuperación<br>3. Mantener una conciencia situacional compartida<br>4. Aumentar la resiliencia | 1. Empoderar a las personas y organizaciones para operar de manera segura.<br>2. Hacer y usar protocolos, productos, servicios, configuraciones y arquitecturas cibernéticas más confiables<br>3. Construir comunidades colaborativas<br>4. Establecer procesos transparentes |

Fuente: Blueprint for a Secure Cyber Future, 2011
Elaborado por: Torres, P. 2020

Pero, estas acciones están apoyadas en el caso del primer objetivo por nueve objetivos más que permitirán que cuando se implementen funcionen en conjunto para anticipar y responder eficazmente a las amenazas, y en el caso del segundo estas acciones están respaldadas por once objetivos que ayudarán a medir el progreso de la construcción de capacidades y determinar si son efectivas ante las amenazas (BSCF, 2011)

## 2.3 Promulgación de iniciativas y estrategias de los Estados Unidos y las Naciones Unidas en la comunidad internacional para operar en el ciberespacio

Especialmente durante la presidencia de Obama las amenazas cibernéticas y los incidentes a las infraestructuras críticas de información en Estados Unidos aumentaron, debido a que, estas amenazas venían de diferentes fuentes, tipos de actores con diferentes capacidades, motivaciones y modos de actuar (Villalba, 2015). Los nuevos adversarios del ciberespacio poseen niveles altos de conocimientos cibernéticos y

cuentan con recursos significativos lo que causa una mayor alarma para los Estados Unidos.

Por lo tanto, desde el 2010 Estados Unidos tuvo la necesidad de crear iniciativas de respuesta a los riesgos y desafíos que se presentan en el ciberespacio, pero esta vez no solo a nivel nacional sino también a nivel internacional. Para esto la administración de Obama creó la "Estrategia Internacional para el ciberespacio" la cual fue publicada en mayo del 2011 este documento plantea por primera vez un enfoque que unifica el compromiso con la comunidad internacional sobre los riesgos que presenta el ciberespacio para todos.

Esta estrategia se propone no solo a ser una visión de EE. UU sobre el futuro del ciberespacio, sino también se estableció como una agenda para ser cumplida con la participación de otros Estados y actores, además, el documento es el contexto para entender las nuevas prioridades de los Estados Unidos en política exterior en el tema de la protección de la seguridad nacional y de cómo impulsar y fomentar acciones en conjunto para reducir amenazas en el ciberespacio. Cuando Clinton presentó la estrategia mencionó que la importancia de esta se basa en crear una visión compartida del ciberespacio para lograr que este sea un lugar abierto, interoperable, seguro y confiable (Bejarano, 2011).

Para Howard Schmidt, el coordinador de ciberseguridad de la Casa Blanca, esta estrategia es mucho más grande que cualquier departamento o agencia ya que, la considera una base sólida para las actividades en materia de ciberseguridad que se realizaran en todo el gobierno y hace una invitación para unir fuerzas con otros países para proteger el ciberespacio del terrorismo cibernético y de los actores con malévolas intenciones (Schmidt, 2011). Estados Unidos también con esta estrategia de cierta manera se proclama líder en el tema de ciberseguridad, porque se compromete a trabajar

a nivel internacional en la creación del futuro del ciberespacio para que sea prospero con mejor seguridad y fiabilidad, que incentive el comercio seguro, la seguridad nacional, la libertad de expresión y la innovación (Rodríguez & Cordero, 2018)

Meses después el Departamento de Defensa (DoD) en julio del 2011 publicó la primera estrategia para operar en el ciberespacio o con su nombre en inglés Strategy for Operating in Cyberspace (SOC), durante el lanzamiento el secretario de defensa William J. Lynn expresó que este plan sirve para poder minimizar el impacto de los ataques cibernéticos (Pellerin, 2011). Este plan señala la importancia de las tareas que realiza el DoD en el ciberespacio, como, por ejemplo, la utilización del ciberespacio para habilitar operaciones militares, de inteligencia, comerciales, movimiento de personal, material y de comando para tener el control de las operaciones militares (SOC, 2011). La iniciativa de este plan también surge de la experiencia con naciones extranjeras y organizaciones de inteligencia transnacionales que ya han intentado entrar en redes clasificadas y no clasificadas del departamento de defensa, y también, reconoce la preocupación de que existan actividades maliciosas en estas redes que aún no han podido ser identificadas (SOC, 2011).

La evolución del internet ha logrado fomentar la colaboración, innovación tecnológica, conectividad, intercambio de información, entre otras más, pero cuando se inició este fenómeno aún no se podía calcular el impacto que esto causaría a las actividades y operaciones del DoD. Por eso, esta estrategia resalta que las bajas barreras de entrada para la actividad cibernética en la actualidad pueden causar grandes daños a los sistemas del DoD específicamente en la economía y en la seguridad nacional de los EE. UU. Debido, a que los actores maliciosos en el ciberespacio están aumentando capacidades cibernéticas a un ritmo acelerado (SOC, 2011).

El DoD está preocupado especialmente en tres áreas específicas que abarca: robo o explotación de datos; interrupción o negación de acceso o servicio que afecte la disponibilidad de las redes, de la información, o de recursos habilitados de la red; y la tercera son las acciones destructivas que incluyen la corrupción, manipulación o cualquier actividad que amenace directamente con destruir redes o sistemas (SOC, 2011). La estrategia desarrollada para operar en el ciberespacio abarca mucho más sobre las preocupaciones del DoD en las cinco iniciativas estratégicas propuestas.

En la siguiente tabla se pueden ver las iniciativas de la estrategia:

*Tabla 2.4 Iniciativas para operar en el ciberespacio del Departamento de Defensa*

| CINCO INICIATIVAS ESTRATEGICAS PARA OPERAR EN EL CIBERESPACIO | |
|---|---|
| ***1.*** Tratar al ciberespacio como un dominio operativo para organizar, entrenar y equipar de esta manera el Departamento de Defensa pueda aprovechar al máximo el potencial del ciberespacio | Al tratar al ciberespacio como un dominio más como el aire, la tierra y el mar, esto le permite al DoD organizar, entrenar y equipar el ciberespacio para los complejos desafíos y las vastas oportunidades del ciberespacio.<br><br>Entre las acciones para combatir el riesgo del ciberespacio el DoD integrará completamente un espectro de escenarios del ciberespacio en ejercicios y entrenamiento para preparar a las Fuerzas Armadas de los EE. UU. y se incluirá equipos rojos cibernéticos por medio de los juegos y ejercicios de guerra. |
| **2.** Emplear nuevos conceptos operativos de defensa para proteger las redes y sistemas de DoD | Implementación de buenas prácticas de higiene cibernética para mejorar la seguridad cibernética<br><br>Se fortalecerá las comunicaciones y la responsabilidad de la fuerza laboral, se realizarán monitoreos internos y se administrarán las capacidades de información.<br><br>Se empleará una capacidad activa de defensa cibernética para evitar intrusiones en las redes y sistemas de DoD y está |

| | |
|---|---|
| | desarrollando nuevos conceptos operativos de defensa y arquitecturas informáticas. |
| **3.** Asociarse con otros departamentos y agencias del gobierno de EE. UU. Y el sector privado para permitir una estrategia de ciberseguridad de todo el gobierno | Se trabajará con otros socios interinstitucionales y con el sector privado para compartir ideas, desarrollar nuevas capacidades, apoyar esfuerzos colectivos para enfrentar los desafíos transversales del ciberespacio y compartir el entendimiento de las necesidades de ciberseguridad. |
| ***4.*** Construir relaciones sólidas con aliados de EE. UU. Y socios internacionales para fortalecer la ciberseguridad colectiva | Este punto apoya a la Estrategia Internacional para el Ciberespacio. Al fomentar la conciencia y alerta situacional compartida permitirá que la autodefensa también sea colectiva. |
| ***5.*** Aprovechar el ingenio de la nación a través de una fuerza laboral cibernética excepcional y una rápida innovación tecnológica | Aprovechar recursos científicos, académicos y económicos para construir un grupo de miembros conformado por personal civil y militar para operar en el ciberespacio.<br>Alta inversión en tecnología, investigación y personal cibernético |

Fuente: Departamento de Defensa (DoD), 2011
Elaborado por: Torres, P. 2020

La Estrategia para Operar en el Ciberespacio se basa en que la seguridad nacional está siendo redefinida por el ciberespacio ya que, en este espacio es donde se encuentran vulnerabilidades para las operaciones militares, de inteligencia y comerciales de EE. UU. Es por eso, que el DoD propuso estas cinco estrategias como un mapa para lograr que las operaciones tengan resultados efectivos en el ciberespacio, para que se defiendan los intereses de la nación y se cumplan los objetivos de seguridad nacional que están contemplados en las Estrategia de Seguridad Nacional (SOC, 2011). Se debe mencionar que cada estrategia es distinta, pero todas se complementan entre sí y las actividades realizadas en cada iniciativa estaban destinadas a que contribuirían al desarrollo de más estrategias por parte del DoD para que EE. UU y sus aliados puedan estar seguros y protegidos en la era de la información (SOC, 2011).

Gracias al avance tecnológico y a la globalización que han creado espacios de oportunidad en los cuales no existen barreras ni límites físicos que fomentan el surgimiento de organizaciones transnacionales con objetivos perjudiciales a la seguridad

nacional mundial. A raíz de esta preocupación la administración de Obama presentó en julio del 2011 "La Estrategia Presidencial para Combatir el Crimen Organizado Transnacional" cuando fue anunciada el presidente Obama dijo que el objetivo de esta estrategia está basado alrededor de un principio único y unificador que es el de construir, equilibrar e integrar las herramientas del poder estadounidense para combatir el crimen organizado transnacional y las amenazas relacionadas a la seguridad nacional y también añadió que es de urgencia invitar a sus socios a tomar las mismas medidas (DHS, 2011).

Para luchar contra el crimen transnacional organizado[5] el plan propone que la manera más efectiva es por medio de una mejor recopilación de inteligencia e intercambio de información en todo el gobierno federal. Dentro de las amenazas del crimen transnacional organizado como el terrorismo, corrupción, lavado de dinero, tráfico de drogas y de personas y otras actividades ilícitas está también considerado el cibercrimen (DHS, 2011). Esta es una estrategia con alcance global que busca que diferentes líderes gubernamentales compartan inteligencia y trabajen juntos para generar resultados efectivos que reduzcan el crimen transnacional organizado no solo en EE. UU sino también en regiones estratégicas en el mundo.

La estrategia promueve cinco objetivos claves para lograrlo:

*Tabla 2.5 Objetivos de la "Estrategia para combatir el crimen Transnacional Organizado" del 2011*

| Cinco objetivos clave de la Estrategia para combatir el crimen Transnacional Organizado |
|---|
| 1. Proteger a los estadounidenses y a nuestros socios del daño, la violencia y la explotación de las redes criminales transnacionales. |

[5] La delincuencia organizada transnacional se refiere a aquellas asociaciones de personas que se perpetúan a sí mismas que operan transnacionalmente con el propósito de obtener poder, influencia, ganancias monetarias, políticas y / o comerciales, total o parcialmente por medios ilegales, mientras protegen sus actividades a través de un patrón de corrupción y /o violencia, o mientras protegen sus actividades ilegales a través de una estructura organizacional transnacional (DHS, 2011)

| |
|---|
| 2. Ayudar a los países socios a fortalecer la gobernanza y la transparencia, romper el poder corruptor de las redes criminales transnacionales y romper las alianzas delictivas estatales |
| 3. Romper el poder económico de las redes criminales transnacionales y proteger los mercados estratégicos y el sistema financiero de EE. UU. De la penetración y el abuso del CTO |
| 4. Derrote las redes criminales transnacionales que representan la mayor amenaza para la seguridad nacional atacando sus infraestructuras, privándolas de sus medios habilitadores y evitando la facilitación criminal de actividades terroristas. |
| 5. Crear consenso internacional, cooperación multilateral y asociaciones público-privadas para derrotar el crimen organizado transnacional.<br>La estrategia también presenta capacidades e herramientas nuevas e innovadoras, que se lograrán priorizando dentro de los recursos disponibles para los departamentos y agencias afectados |

Fuente: Obama White House Archives, 2011
Elaborado por: Torres, P. 2020

Esta estrategia es un complemento a las otras iniciativas importantes en el ámbito de la seguridad de EE. UU, pero, está guiada especialmente por la Estrategia de Seguridad Nacional y en el tema de cibercrimen también se entrelaza con la Estrategia Internacional para el Ciberespacio (HSDL, 2011). En lo que respecta al cibercrimen esta estrategia menciona el alto costo financiero que produce al Estado las amenazas a las redes informativas gubernamentales y corporativas, es por eso que la tarea conjunta nacional de investigación cibernética, dirigida por la Oficina Federal de Investigaciones (FBI) trabaja para 18 agencias o departamentos federales para coordinar, integrar y compartir información relacionada con investigaciones sobre amenazas cibernéticas y del mismo modo trabajando para que el internet sea un lugar seguro para perseguir a los actores que buscan afectar y explotar los sistemas estadounidenses (HSDL, 2011).

Tomando en cuenta el contexto global en que se encuentra el ciberespacio se debe hacer mención a que la Organización de la Naciones Unidas (ONU) por medio de la Unión Internacional de Telecomunicaciones (UIT), la agencia especializada en las TIC que es la responsable de temas de ciberseguridad. Esta agencia promueve la cooperación internacional, debido, a que de igual manera que los Estados Unidos mira a las amenazas cibernéticas como una amenaza de alcance global, es por eso, que es

necesario unir fuerzas y actuar multilateralmente en asuntos críticos para reforzar y crear alianzas estratégicas (ITU, 2007).

Entre las iniciativas principales de esta agencia se encuentra la "Agenda Global de Ciberseguridad" con sus siglas en inglés (GCA) que fue lanzada en el 2007. Esta agenda es básicamente un marco de cooperación internacional para mejorar la seguridad de la información trabajando sobre las iniciativas existentes para evitar la duplicación de esfuerzos entre los socios interesados (ITU, 2007). La Conferencia Mundial de la UIT y la de Plenipotenciarios del 2010 fortaleció e incrementó el papel de esta organización en el tema de la ciberseguridad, por eso es, relevante mencionar que la GCA de ese año se enfocó en las crecientes amenazas de ciberseguridad y por medio de este marco propuso respuestas muy similares a las que EE. UU propuso con su Estrategia Internacional para el Ciberespacio y sus otros planes que fueron anteriormente mencionados (ITU, 2011).

Por otro lado, la ONU en conjunto con un grupo de quince expertos gubernamentales en el campo de la información y las telecomunicaciones desarrolló reportes que fueron presentados en la sexagésima octava sesión de la Asamblea General. Los cuales contienen recomendaciones para promover seguridad internacional, paz y estabilidad en el uso de las TICS. El reporte del 2010 resalta que la cooperación internacional es un factor principal para reducir riesgo y aumentar la seguridad, también, se destaca el aparecimiento de numerosas iniciativas multilaterales, regionales y bilaterales desde el 2010 lo que incrementó notablemente la importancia hacia la ciberseguridad y el correcto uso de las TIC (ONU, 2013).

Las crecientes amenazas por el desarrollo y difusión de nuevas herramientas en las redes aumentan el riesgo para los Estados. Por lo tanto, por medio de estas recomendaciones se espera que se logre un entendimiento común entre los Estados para que todos tengan un comportamiento adecuado con respecto al uso de las TIC (ONU,

2013). Además, de que la ONU se compromete a liderar mesas de diálogo entre los Estados miembros para incentivar la cooperación, el mejor entendimiento y apoyar la creación de nuevas iniciativas.

El avance tecnológico en los últimos años ha crecido de manera inesperada lo cual también, ha traído desafíos y amenazas a la seguridad nacional de las naciones. Por ese motivo, en este capítulo se cumplió con el objetivo de describir las respuestas por parte del gobierno de Obama y de la ONU frente a los desafíos e inseguridad que se presentan en el ciberespacio por la participación de actores no estatales. Es por eso que se describió específicamente en el caso de los Estados Unidos sus iniciativas, planes y estrategias más relevantes durante el período de estudio para fortalecerse, asegurase y aumentar su ciberseguridad en el ciberespacio. Por la gran influencia que tiene esta nación en la comunidad internacional se incluyó los esfuerzos en ciberseguridad implementados por la ONU en los cuales se puede ver la gran similitud de sus iniciativas con las que fueron planteadas por los EE. UU.

En el caso particular de los Estados Unidos y en el gobierno de Barack Obama se evidenció en como la ciberseguridad paso a ser tema principal en la agenda política nacional e internacional ya que, la dependencia al ciberespacio está incrementando constantemente, lo que se convierte en una prioridad dominar este nuevo escenario para evitar que la seguridad nacional y el poder económico y político de los EE. UU se encuentre en peligro.

El empoderamiento y oportunidades que presenta el ciberespacio para los diferentes tipos de actores genera preocupación a gran escala para los gobiernos ya que, es evidente que el internet puede incrementar capacidades y las asimetrías de poder entre Estados y actores no estatales se vuelven menos notorias, lo que causan amenazas que pueden llegar a desestabilizar el orden internacional. Es por eso, que en el siguiente

capítulo se explorará más a fondo la relevancia de WikiLeaks como un actor transnacional y sobre como sus acciones han despertado el interés y la necesidad urgente de incrementar capacidades cibernéticas en los Estados Unidos para evitar que filtraciones, ataques, robo de información, espionaje entre otras acciones peligrosas vuelvan a suceder.

## 3. Capítulo III: WikiLeaks un nuevo actor influyente del ciberespacio en la transformación de la dinámica del poder de los Estados Unidos en las relaciones internacionales

En este capítulo se busca reconocer y resaltar la relevancia del ciberespacio y de los actores transnacionales en las relaciones internacionales tomando en cuenta la actuación de WikiLeaks y las repercusiones que surgen por su aparición y participación en el escenario internacional. La creciente dependencia al ciberespacio por parte de los Estados se ha venido convirtiendo en una preocupación de seguridad nacional, especialmente para los Estados Unidos que lo ha reiterado en sus declaraciones sobre las amenazas y peligros que representa el ciberespacio a su seguridad, por eso, resalta el rol de incrementar estrategias de ciberseguridad para operar en el ciberespacio.

El caso de WikiLeaks en el ciberespacio muestra que hay cambios en el poder dentro de este dominio, la emergente aparición de grupos de cierta manera disidentes como WikiLeaks pone en alarma al Estado que para defenderse debe tomar medidas represoras que bajo este contexto de ciberespacio, estas, medidas son estrategias para emplear ciberpoder[6], es decir, según el autor Joseph Nye el ciberpoder depende de los recursos que caracterizan el dominio del ciberespacio (Nye, 2010, p.3). Además, resalta la importancia de la combinación del poder duro y blando con recursos cibernéticos para ejercer control dentro de este espacio relativamente nuevo en donde, los Estados recién comienzan a entender los desafíos que conlleva el avance tecnológico y la alta dependencia al ciberespacio (Nye, 2010, p.7).

A lo largo de este capítulo se va abordar las acciones de los Estados Unidos frente al ciberespacio como un dominio de carácter global que está al alcance de todos los individuos con acceso a internet. El internet por sus características de fácil acceso, de

[6] Ciberpoder: Es la habilidad de obtener resultados esperados por medio del uso de recursos de información que están interconectados electrónicamente al dominio cibernético (Nye, 2010, p.4)

reducción de temporalidad, transcender barreras físicas que facilitan y empoderan a los individuos de maneras inimaginables, son razones suficientes para que el ciberespacio se convierta en una amenaza directa para el gobierno estadounidense, que para aumentar capacidades cibernéticas tiene la urgente necesidad de impulsar ciberpolíticas, aumentar presupuestos en ciberseguridad y crear instituciones que trabajen completamente en aumentar las capacidades cibernéticas para garantizar la seguridad de la nación y aumentar su poder para tratar de ejercer control dentro de este nuevo dominio (Armstrong, 2015, p. 34).

### 3.1 El ciberespacio como un lugar estratégico para el surgimiento y empoderamiento de actores transnacionales como WikiLeaks y como su actuación repercute en el juego de poder

A finales del siglo XX y principios del siglo XXI la globalización impulsó la revolución de las comunicaciones, un fenómeno que surgió gracias al Internet una herramienta que sus orígenes se encuentran en una red de computadora ARPANET que fue creada en 1969 por la Agencia de Proyectos de Investigación Avanzada (ARPA) del Departamento de Defensa de los Estados Unidos, con el fin de compartir información interna entre el departamento (Nardoianni, 2016, p.49). Sin embargo, cuando los investigadores de ARPA crearon esta red no había manera en que se hubiesen podido imaginar el impacto que tendría su creación en el futuro de la sociedad.

El Internet nos conlleva a un nuevo espacio virtual construido por la interacción humana con la tecnología, que es conocido como el ciberespacio en donde no existen barreras físicas (Sigholm, 2013, p. 2). Este nuevo espacio ha sido identificado por los Estados como el quinto dominio además de la tierra, mar, aire y el espacio ya que, también, es un nuevo espacio en donde se pueden emplear operaciones militares para defenderse de las amenazas (Sigholm, 2013, p. 2). Debido, a que en los últimos años

han surgido desafíos y amenazas inesperadas. Estos eventos recientes han mostrado el rol que ocupan los actores no estatales, en el ámbito de que son capaces de causar daños, retos y, por lo tanto, preocupación a los Estados que están cada vez más altamente dependientes al ciberespacio, por eso, consecuentemente el internet se convierte en un desafío enorme para los Estados en la gobernanza internacional (Azócar & Lavín, 2015, p. 1). Especialmente para el caso de los Estados Unidos que depende de los servicios del Internet para llevar acabo sus operaciones críticas (Nardoianni, 2016, p.49).

La importancia y la dependencia del ciberespacio en la sociedad moderna ha venido creciendo notablemente, por ejemplo, en los últimos años desde el 2000 que el internet estaba en sus inicios solo hasta el 2010 el uso global del internet se incrementó el 500% creciendo entre 350 millones a 2 billones de usuarios en internet (Sigholm, 2013, p. 2). Por lo tanto, mientras más personas estén cada vez más interconectadas por internet, esto hace que el análisis sobre el cómo actuar en el ciberespacio antes los diferentes tipos de amenazas que pueden surgir se vuelve más complicado dentro de este nuevo escenario de participación internacional (Azócar & Lavín, 2015 p. 3).

Este nuevo escenario de participación internacional se caracteriza por su naturaleza asimétrica, reducción de costos de acceso, ambigüedad legal, lo que representa un empoderamiento significativo para los actores no estatales ya que, por medio, de estas herramientas pueden lograr ataques efectivos a corto plazo (Gomes de Assis, 2017). Para Nye (2014) esta apertura y popularización de la tecnología tiene innegables implicaciones políticas, debido a que el fácil y barato acceso al internet puede llevar a un posible cambio en la balanza de poder. Por una parte, promueve la reducción del poder entre los Estados y por otra, los actores no estatales como los individuos y organizaciones transnacionales tienen la posibilidad de incrementar

capacidades que los empoderan y de esta manera es posible su participación dentro del ciberespacio a través de transmitir y difundir información (Azócar & Lavín, 2015, p. 4).

En el caso de WikiLeaks como actor transnacional que se ha caracterizado por difundir información confidencial de interés sobre Estados y corporaciones, con esto ha logrado durante sus publicaciones entre el 2009 al 2010 establecer acciones coordinadas para incidir en asuntos internacionales (Azócar & Lavín, 2015, p. 4). La organización WikiLeaks se la puede considerar como un grupo de hackers con sentido social, conocido con el nombre de hacktivistas[7], es decir, es un grupo de individuos que hacen uso de los recursos del ciberespacio para generar protestas, promover alguna ideología, e impactar en las agendas políticas (Sigholm, 2013, p. 14). Entonces, WikiLeaks empata en esta categoría como una organización de hacktivistas ya que, entre las principales herramientas que utilizan son: desfiguraciones de los sitios web, ataques de denegación de servicio, robo de información, parodias de sitios web, y otras diversas formas de ciber sabotaje (Sigholm, 2013, p. 14).

Por consiguiente, WikiLeaks con sus acciones hacktivistas y anti hegemónicas contra EE. UU en el ciberespacio logró alcanzar un estatus de influencia e impacto por medio de acciones de comunicación pública, la cual, es la principal actividad de un actor no estatal para ejercer poder de influencia. En este caso, este tipo de poder está determinado por la percepción de la legitimidad y la representación que obtengan (La Porte, 2016, p.8). No obstante, el internet puede ser usado como una herramienta articuladora entre actores estatales que siguen teniendo el protagonismo en la política, pero ven la necesidad de prestar atención a grupos civiles que están expuestos a la

[7] El hacktivismo es el uso de recursos del ciberespacio, de manera legal o (quizás más comúnmente) ilegal (Sigholm, 2013, p. 14)

influencia transnacional de diferentes actores que transmiten sus objetivos, ideales y valores sobre asuntos internacionales (Azócar & Lavín, 2015, p. 4).

Es por eso, que este rol articulador del internet se asocia con un tipo de presión ejercida por los diferentes actores no estatales que va desde abajo hacia arriba (Azócar & Lavín, 2015, p. 5). El caso de WikiLeaks es una muestra contundente del poder de articulación que llegan a tener los actores no estatales, la revelación de los cables diplomáticos provocó una situación conflictiva en las diferentes embajadas que en algunas desencadenó más tensiones que en otras, pero también, desató protestas hacia gobiernos corruptos, empresas que ejercían malas prácticas ambientales, bancos que apoyaban la evasión de impuestos entre otras situaciones que WikiLeaks logró sacar a la luz (Conde, 2014, p.17).

Es por estos acontecimientos que se puede afirmar que el ciberespacio ha proporcionado el lugar ideal para que actores no estatales puedan causar disrupción en el orden internacional, estos efectos disruptivos se pueden notar a través de la variedad de iniciativas para proteger la infraestructura informática, sistemas financieros y la seguridad nacional de los países (Azócar & Lavín, 2015, p. 7). WikiLeaks con sus filtraciones a gran escala ejerció en su momento un rol disruptivo al intentar estos ataques para generar cambios en las estructuras de poder por medio del uso de la información, la organización es una muestra de cómo los grupos o individuos pueden causar situaciones críticas alarmantes desde un computador (Azócar & Lavín, 2015, p. 7).

Estados Unidos se ha mostrado como una nación pionera en innovación tecnológica y que a raíz de los sucesos ha reforzado sus capacidades. En la actualidad según el Índice Global de Ciberseguridad de la UIT que mide el desarrollo de capacidades cibernéticas del 2019. Estados Unidos ocupa el puesto número dos en el

top de los países con mejor ciberseguridad en el mundo después del Reino Unido (Bowman, 2019). Los altercados que han ocasionado WikiLeaks o el caso de Edward Snowden han servido para que Estados Unidos se mantenga enfocado en incrementar ciberseguridad para evitar que la información de contenido sensible vuelva a ser expuesta.

Por ejemplo, en los casos mencionados anteriormente tenemos a WikiLeaks que entre sus fuentes para una de sus más controvertidas publicaciones logró conseguir información por medio de un *cyber-insider* que se refiere a actores que cuentan con acceso legitimo a las redes, sistemas y por lo tanto a la información que se encuentra almacenada en estas, pero son actores que actúan de manera desleal con su empleador y los traicionan por obtener beneficios económicos o son impulsados por otras motivaciones (Sigholm, 2013, p. 17). De igual manera Edward Snowden fue un ex empleado de la CIA y la NSA, pero en 2013 decidió hacer público documentos clasificados sobre los programas de vigilancia y espionaje masivo que empleaba el gobierno estadounidense (Conde, 2014, p.142). Dados estos casos la Agencia de Proyectos de Investigación Avanzada de Defensa (DARPA) de los EE. UU identificó estas amenazas y elaboró un proyecto llamado "*The Cyber Insider Threat*" conocido como CINDER (Sigholm, 2013, p. 17) para detectar oportunamente este tipo de actores maliciosos que operan con menos dificultad en las redes del gobierno.

La importancia creciente del ciberespacio radica en que está conformado por nuevos recursos tecnológicos que causan vulnerabilidad y surgen diferentes tipos de amenazas cibernéticas, que por la constante innovación tecnológica se vuelven amenazas cada vez más especializadas y difíciles de identificar, lo que, causa que los Estados alcancen nuevas dimensiones en seguridad nacional (Choucri, 2013, p. 223). El ciberespacio también presenta nuevos tipos de asimetrías entre los Estados, esto brinda

la oportunidad para que actores estatales más débiles influyan o incluso amenacen a Estados más fuertes, o actores no estatales amenazando a Estados, también, se pueden ver refiere a la simetrías que se capacidad de los Estados para entrar en las redes de otros Estados (Choucri, 2013, p. 224). Cualquiera que sea el caso es una muestra del cambio de juego del poder (Choucri, 2013, p. 224).

La actuación de WikiLeaks en el 2010 fue vista por los Estados Unidos como una de las mayores crisis de seguridad que les había tocado enfrentar, este suceso mostró la politización y la disrupción del ciberespacio (Choucri, 2013, p. 224). Las respuestas hacia las publicaciones de WikiLeaks fueron diferentes en distintas partes del mundo, pero en general la mayoría de los Estados aunque no hayan sido involucrados en las publicaciones vieron a la organización y a sus acciones como una amenaza directa a la soberanía y a la seguridad nacional, por lo que, la actuación de WikiLeaks fue relevante ya que, los Estados se concientizaron sobre la importancia de desarrollar medidas preventivas y aumentar capacidades cibernéticas para protegerse en el ciberespacio (Choucri, 2013, p. 225).

### 3.1.2 Estado del arte del poder blando

Esta nueva categoría del poder en las relaciones internacionales fue planteada por Joseph Nye en su libro *The changing nature of American power* en 1990, en el cual surgieron las primeras ideas del *soft power* o poder blando, que hace referencia a las capacidades que tiene un Estado para influenciar en los intereses y acciones de otros Estados por medio de factores o elementos culturales e ideológicos que promuevan valores que son legitimados por los otros actores estatales del sistema internacional (Morales, 2012, p.2). En el año 2004 Nye publicó *Soft power and Power in Global Information Age: The Means to Success in World Politics*. En donde surgió la

definición: *Soft power is the ability to get what you want by attracting and persuading others to adopt your goals. It differs from hard power, the ability to use the carrots and sticks of economic and military might to make others follow your will* (Torres, 2018, pg. 17).

Es decir, el *soft power* se basa en la habilidad que tiene un actor estatal para estructurar una situación para que otros actores desarrollen preferencias o definan sus intereses, de tal, forma que concuerden con los intereses del Estado predominante. Para el autor Joseph Nye este poder proviene de elementos atrayentes como la cultura, ideología, valores políticos (externos e internos), política exterior (legitima y con moral) y por influencia de regímenes internacionales extranjeros (Morales, 2012, p.2).

En el caso de los Estados Unidos según Nye es considerado como uno de los países que tiene mayores capacidades de poder blando como también poder duro. Sin embargo, este país no ha sido el creador de esta categoría de poder, pero si lo ha empleado a lo largo de los últimos años ya que, el uso del poder blando para el autor coincide en que se ha dado en conjunto con el surgimiento de un nuevo orden internacional que está regido por la globalización (Morales, 2012, p.2). Es importante mencionar que el poder suave no es algo que solo los Estados Unidos lo ha venido recientemente implementando, sino que también, existe evidencia de que a finales del siglo XIX Francia intentó promover su cultura por medio del lenguaje, literatura y arte para lo que formó una Alianza Francesa, de igual manera, en tiempos de la Alemania Nazi se utilizó a la propaganda por diferentes medios de comunicación para implantar y expandir la ideología de igual manera la URSS expandió e influyó con la ideología comunista  a otras naciones en el mundo (Morales, 2012, p.3).

En la actualidad se debe tomar a la globalización con un factor relevante ya que, sin ella el poder blando no pudiese tener el impacto que ha logrado en la cultura,

costumbres e ideologías de las personas (Torres, 2018, pg. 11). Sin embargo, a lo largo de los últimos años los elementos de poder han cambiado para los Estados modernos según Nye no basta que un Estado, solo hago uso de herramientas de poder blando, sino que también debe fusionar con el uso de herramientas de poder duro modernas para así tener un *Smart power* (Torres, 2018, pg. 14). Es decir, una estrategia inteligente que ayude a mantener y conservar el poder en el sistema internacional. Para comprender mejor que fuentes corresponden al poder duro y suave se puede ver en el siguiente listado:

*Tabla 3.1 Fuentes de poder duro y blando de un Estado moderno*

| Fuentes Poder Duro | Fuentes de Poder Blando |
|---|---|
| • Economía<br>• Tecnología<br>• Poder Militar | • Valores políticos<br>• Cultura<br>• Política exterior |

Elaborado por: Torres. P, 2020
Fuente: Nye, 1990

Dentro de las herramientas de poder blando se debe resaltar la importancia de cultura para generar atracción. La cultura está dividida en la alta cultura que es la que abarca elementos como: arte, literatura, valores, educación, ideales, por otra parte, la otra división es la cultura popular que la que contiene a la industria del entretenimiento, y la promoción de valores universales, es por esto, que Nye considera a la cultura como un poderoso medio de influencia (Torres, 2018, pg. 20). Sin embargo, este elemento no es el único que crea *soft power*, otros recursos como la información, conocimiento y la interdependencia han venido tomando relevancia e impacto dentro del *soft power* y en las relaciones internacionales (Yukaruc,2017, p.4).

Tomando al elemento de la política exterior como fuente de poder blando este se relaciona directamente con la diplomacia que se ha convertido en un vehículo este

poder, gracias a la innovación tecnológica el uso de la diplomacia en la actualidad no está solo bajo el control del Estado, sino que, ha pasado a llamarse "diplomacia pública" (Yukaruc,2017, p.4). La cual, se han venido incrementado debido a que las tecnologías de la comunicación con el desarrollo del internet han logrado facilitar que diferentes y diversos actores puedan generar e intercambiar información sobre diferentes temáticas mundiales que afectan la manera en que se puede observar a un Estado (Yukaruc,2017, p.4).

No solo los Estados Unidos es un ejemplo del uso de estrategias de poder blando en las relaciones internacionales, sino que, por el nuevo orden de gobernanza mundial impulsado por la globalización, también, diferentes Estados se han visto llamados a hacer uso de tácticas de poder blando (Morales, 2012, p.3). Nye, también se ha destacado por estudiar e identificar estrategias de poder blando en diferentes naciones, por ejemplo; Japón para el autor se destaca entre los países asiáticos por el mantenimiento de su cultura única y cómo esto ha influido a que ocupe el primer lugar en el mundo por la mayor cantidad de patentes y ocupa el segundo puesto en ser el país en mayor venta de libros y música (Morales, 2012, p.3). Entre otros países con poder blando esta España que entre sus fuentes de poder sobresale el idioma especialmente en las relaciones con sociedades que históricamente son afines como el caso con América Latina (Morales, 2012, p.4).

El poder blando en el caso de Brasil ha sido utilizado para su inserción internacional mediante el uso de valores políticos y por sus atractivos culturales (Carnaval brasileño, fútbol) para así desviar la atención a sus problemas internos como la desigualdad social, violencia y corrupción (Morales, 2012, p.5). En el caso de Rusia se observa al poder blando en tres facetas: obtención de legitimidad política, interdependencia económica y valores culturales, estas facetas se pueden notar en el

liderazgo político en la creación de instituciones regionales, atracción cultural por medio de promoción del idioma, y por la propagación de medios de comunicación rusos (Morales, 2012, p.8).

Por último, el poder suave en China según Nye el resalta los aspectos culturales de China y la fama mundial que ha logrado por medio de diferentes reconocimientos a nivel mundial como premio el Nobel en literatura, cine, deportistas chinos, además, de que China en el ámbito de la educación ha motivado a miles de estudiantes extranjeros a estudiar y trabajar allí, también ha creado Institutos Confucianos alrededor del mundo y una radio china internacional en idioma ingles emitiendo las 24 horas del día (Morales, 2012, p.8).

Como se ha podido evidenciar en el desarrollo del estado del arte del poder blando, este tiene pocos años desde su reciente conceptualización por Joseph Nye, esto ha generado algunas críticas. Desde una perspectiva comunista esta idea del poder suave es criticada ya que, emerge desde el liberalismo que no toma en cuenta las clases sociales, pero Nye ha enfatizado que esta categoría no encaja con el pensamiento liberal o idealista simplemente es una forma de poder para obtener resultados deseados (Morales, 2012, p.3). Entre otras de las críticas que se resaltan sobre el poder blando es que no es un concepto original y nuevo, sino que presenta similitudes con otros enfoques y teorías de las relaciones internacionales (Yukaruc,2017, p.6).

Desde la perspectiva del realismo clásico de Carr se puede asociar su concepto de poder con el poder blando e inteligente de Nye; debido, a que Carr divide al poder en tres categorías: militar, económico, y el poder sobre la opinión, es por eso, que la combinación de estos elementos sirve para ejercer control y obtener seguridad por lograr el cambio de comportamiento en las acciones de otros Estados (Yukaruc,2017, p.6). Además, Carr destaca que elementos intangibles como la psicología humana, la

opinión pública y la persuasión juegan un rol importante dentro del poder ya que, es importante que un líder pueda tener acceso a estas herramientas para ejercer un "poder inteligente" dentro de lo que se conoce en la concepción de Nye (Carr, 1946, p. 132). Por consiguiente, para Carr como un representante del realismo clásico resalta la importancia de los recursos tangibles del poder como el militar y económico, pero también, coincide en que se debe fusionar ambos elementos del poder para obtener mejores resultados (Yukaruc,2017, p.6).

Otro enfoque similar al de Nye viene por parte de Steven Lukes en su obra Power: A Radical View en 1974, en el cual definió tres dimensiones del poder: la primera se refiere a que A puede ejercer poder sobre B haciendo que haga lo que no quiere hacer, pero también ejerce poder sobre él al influir, moldear o determinar sus propias necesidades " (Lukes, 1974, p. 23). En la segunda dimensión el autor explica que esta manera A evita conflictos con B ya que, hace creer a B que sus preferencias se moldearon bajo ninguna presión externa y que son preferencias propias. Por lo que, en esta dimensión resalta la importancia del control de la información, de los medios de comunicación y de los procesos de socialización (Yukaruc,2017, p.7). La tercera dimensión hace referencia a como los individuos naturalizan este proceso y rol de control, esta dimensión es en la que el ejercicio de poder es más notorio ya que, según el autor este control del pensamiento es considerado el ejercicio de poder más supremo e insidioso que se puede ejercer (Yukaruc,2017, p.7). Se debe resaltar también, que esta dimensión se asimila al poder blando que se basa en la atracción y en el objetivo de afectar y cambiar las preferencias y percepciones de los otros.

Por otra parte, se asocia al poder blando con el concepto de hegemonía que propuso Antonio Gramsci. Para comprender mejor esta asociación primero se debe entender que el pensamiento de Gramsci viene de la corriente marxista, en la cual,

desarrolló su concepto de hegemonía que refiere a la importancia de la participación de la sociedad política y civil, debido a que, la hegemonía necesita “la combinación de fuerza y consentimiento, que se equilibran recíprocamente sin que la fuerza predomine excesivamente sobre el consentimiento" (Gramsci, 1971, p.80). Por lo tanto, para el autor fue importante analizar como las clases sociales burguesas usaban a las esferas privadas y civiles para justificar, mantener el poder y reproducir el modelo de dominación por medio del consentimiento de los subordinados, a través del uso de la cultura creando el concepto de hegemonía ideológica o cultural (Albarez, 2016, p. 3).

Para Gramsci la hegemonía se filtraba por la cultura que especialmente era transmitida por la esfera social privada como; la iglesia, instituciones educativas, partidos políticos y medios de comunicación los cuales se encargan de crear y reproducir valores e ideologías que llegan a ser normalizados entre los otros actores civiles de una sociedad (Yukaruc,2017, p.7). Es por eso, que tener la dirección cultural de la sociedad permite a la clase dominante fortalecer y consolidar su predominio, por medio del liderazgo intelectual y moral que permite utilizar el consentimiento y la persuasión en lugar de la coerción para mantener el poder (Albarez, 2016, p. 4). En base a esto, Gramsci resalta el rol de los intelectuales que son los encargados de ayudar a las clases sociales dominantes a formar estructuras de conocimiento y sistemas de valores sólidos. Además, no solo los intelectuales son los encargados de crear estas estructuras, sino que también, ellos llevan estos intereses a las clases subordinadas transformados en concepciones universales para que estas acciones lleguen a tener un consentimiento general por la sociedad (Yukaruc,2017, p.7).

La similitud del enfoque del poder blando de Nye con la hegemonía cultural de Gramsci está en que ambos enfoques demuestran la importancia que tiene lograr consentimiento sobre ejercer cohesión para lograr objetivos. Además, de que Gramsci

por un lado destaca el rol de la cultura para mantener la hegemonía, por medio, del rol de intelectuales, educación, la iglesia, medios de comunicación entre otros, por otro lado, Nye utiliza a estos elementos como fuentes de poder blando (Yukaruc,2017, p.7).

El estudio del poder y de la hegemonía es realmente amplio, tomando ahora un perspectiva realista y liberal en las relaciones internacionales surge por primera vez en 1973 la Teoría de Estabilidad Hegemónica por Charles Kindleberger, que fue el que le dio un enfoque liberal ya que, se dedicó a estudiar las causas de la gran depresión de 1929-1939 obra en la cual concluyó que la crisis económica se debe a que en ese tiempo hubo una falta de liderazgo y declive en la hegemonía por parte de Gran Bretaña y sus aliados en el sistema económico y monetario internacional, lo que causó toda esa inestabilidad económica en el sistema internacional, es decir, el factor del liderazgo para Kindleberger es fundamental para que sea posible mantener la estabilidad que da el libre comercio (Herrera, 2017, p.18).

La teoría fue retomada e impulsada principalmente por Robert Keohane y Robert Gilpin (1987), estos dos autores definen que dentro de un orden económico liberal mundial una nación obtiene hegemonía cuando es un Estado preponderante en recursos materiales, que con ellos logra ejercer control sobre materias primas, mercados, capital, tiene ventaja competitiva en la producción de bienes lo que hace que este liderazgo fomente y estabilice el sistema de libre comercio (Navarro, 2009, p. 12), Además, la idea principal de esta teoría se basa en que para tener un sistema internacional estable debe existir un único actor dominante que tenga la capacidad de generar resultados colectivos deseables, en caso de que no exista un Estado hegemón esto causará desorden y anarquía que conlleva a resultados negativos para todos los Estados en el sistema internacional (Herrera, 2017, p.20).

En lo que compete al aporte de Keohane en esta teoría, este autor hace una relación de la hegemonía con la interdependencia compleja la que se caracteriza por tres procesos: surgimiento de canales múltiples que conectan a las sociedades por medio de relaciones transnacionales, transgubernamentales de tipo económicas y sociales; ausencia de jerarquía en temas de moldear la agenda internacional; y la última sobre la reducción del uso de fuerza militar entre Estados con relación de interdependencia (Herrera, 2017, p.22). Keohane, considera que no solo la concentración de recursos materiales es suficiente para la estabilidad de una hegemonía, sino que, es necesario que el Estado hegemón tenga voluntad y capacidad de ejercer liderazgo para producir reglas, instituciones, regímenes que fomenten la cooperación entre los Estados (Herrera, 2017, p.23).

Además, Keohane resalta que es importante el prestigio ideológico lo que hace que los otros Estados también se alineen con este pensamiento y puedan lograr intereses comunes, en este punto se puede asociar con la visión gramsciana ya que, Keohane adopta una parte de este pensamiento cuando afirma que la consolidación de una hegemonía se da siempre y cuando sea aceptada por los otros Estados que han reconocido a esta hegemonía como algo benéfico para mantener el orden internacional (Herrera, 2017, p.23). Esta teoría de la estabilidad hegemónica como ha sido remodelada también destaca el uso de las fuentes de poder blando para mantener y consolidar una hegemonía.

Se ha realizado una revisión sobre el estado del arte sobre el poder blando y las diferentes perspectivas existentes sobre el poder y la hegemonía. Con el desarrollo y revisión de literatura del poder blando se ha podido encontrar que los recursos de este poder no son totalmente originales y creados exclusivamente por Nye ya que, en otras teorías se ha visto que diferentes autores han planteado puntos muy similares con el

concepto de poder blando y sus herramientas. Sin embargo, para el desarrollo de esta investigación en el marco teórico se ha decidido tomar el enfoque del poder blando de Joseph Nye debido, a que es un autor que ha profundizado más esta temática en las relaciones internacionales referente a la globalización y las tecnologías.

Especialmente con el caso de los Estados Unidos y la globalización en la era de la información en donde ha contribuido con más conceptos para el poder en una época moderna, lo que, hace más relevante a este enfoque para el desarrollo de la presente investigación. Además, se debe mencionar que Nye no considera al poder blando como una teoría de las relaciones internacionales, sino que, es más bien un enfoque analítico que encaja con diferentes visiones que van desde las perspectivas realistas hasta las constructivistas.

### 3.1.3 Estrategias de poder blando y duro implementadas por los Estados Unidos en el ciberespacio frente a la aparición de WikiLeaks

Como ya se ha mencionado anteriormente sobre la virtud que posee el ciberespacio de empoderar inimaginablemente a los individuos para desafiar a los conceptos tradicionales de la soberanía. El ciberespacio es un lugar de participación abierto en donde los puntos de control pueden ser compartidos, lo que, produce que las relaciones y la naturaleza del poder se encuentre en constante transición (Choucri, 2013, p.14). Es por eso, que los recursos de poder están cambiando debido a factores como: la tecnología, innovación, el crecimiento económico y educación que en la actualidad se están volviendo más importantes, que las zonas geográficas, número de población, recursos materiales y naturales entre otros factores tradicionales que se están perdiendo relevancia (Nye, 1990, p. 55)

Desde la década de los noventa para el autor Joseph Nye era importante entender que la naturaleza del poder con el paso del tiempo estaba en constante cambio, y que las

maneras de ejercer poder no solo podían ser asociadas por la posesión de ciertos recursos tangibles, sino que existían otras maneras o recursos para ejercerlo (Nye, 1990, p. 56). Nye propuso dos categorías para el poder que las llamó: poder duro y poder blando. El poder blando es la habilidad de establecer preferencias, ideas, es decir, todo lo que esté relacionado con recursos intangibles para lograr establecer una agenda política que se adapte a los intereses y preferencias, a diferencia del poder duro que se asocia tradicionalmente con recursos tangibles como el crecimiento económico, armamento militar, territorio, recursos naturales entre otros (Nye, 1990, p. 56).

El siglo XXI está marcado por ser una época de constante innovación, desarrollo y crecimiento tecnológico. Es por eso, que es una era de información e interdependencia transnacional ya que, el poder es más transferible, se vuelve más intangible y menos coercitivo (Nye, 1990, p. 57). Para Nye el poder tiene cuatro características esenciales: agencial; conductual; relacional; contextual (Masullo, 2011, p.8). De estas sobresale el contexto, es por eso, que desde los sucesos del 9/11 los que marcan el inicio de un nuevo contexto internacional en donde la globalización y la información tienen un rol predominante que terminan incidiendo en la transformación del poder en dos facetas: transición y difusión (Masullo, 2011, p.8). La transición se refiere al movimiento del poder entre un Estado hegemónico a otro particularmente la transición de poder de "occidente a oriente", la segunda faceta se refiere al movimiento del poder de los Estados a actores no estatales (Masullo, 2011, p.11).

La segunda faceta de la transformación del poder resulta más novedosa, debido, a que la difusión del poder trae ventajas y desventajas. Por una parte, ayuda a la propagación de recursos de poder blando a las diferentes sociedades, por la otra, pone a disposición de actores no estatales, tales como empresas, grupos terroristas transnacionales y cibernéticos diversos recursos de poder blando y duro lo que aumenta

sus capacidades para actuar y afectar negativamente (Masullo, 2011, p.11). Es por este motivo, que Nye resalta la importancia del poder blando y el rol de la difusión en la revolución de la información ya que, esta revolución ha permitido que surjan nuevos actores con recursos de poder blando cada vez más sofisticados acorde a la innovación y al contexto internacional, lo que les dará mayores posibilidades de formar alianzas y de potenciar su participación (Masullo, 2011, p.11).

Como se hizo mención anteriormente para Nye el poder depende del contexto por lo que el ciberespacio es un contexto de mucha importancia para la política internacional. Especialmente para los Estados poderosos como EE. UU que ha logrado el control de los otros dominios, el ciberespacio se vuelve un verdadero reto ya que, es evidente por los sucesos ocurridos a lo largo de la década que estos eventos están por fuera del control de los Estados (Choucri, 2013, p.13). Sin embargo, esto no quiere decir que los Estados ya no son los actores dominantes esto no ha cambiado, pero, lo que si se debe reconocer es que es un escenario lleno de diferentes tipos de actores lo que hace que se vuelva difícil ejercer control (Nye, 2010, p.5)

WikiLeaks es un actor relevante porque ha usado a la información como un arma de ataque hacia los poderes establecidos, el rol de la información es fundamental ya que, es una fuente directa de poder (Gomes de Assis, 2017). A lo largo de los años los gobiernos del mundo se han preocupado por mantener el control de la información, pero por el avance tecnológico se producen cambios dramáticos para este elemento intangible de poder. Se debe recalcar que el poder basado en recurso de información no es algo nuevo pero debido a las circunstancias actuales emerge un nuevo poder con el nombre de poder cibernético (Nye, 2010, p.7). Este poder se refiere a la habilidad de usar el ciberespacio para obtener ventajas, resultados anhelados e influir en otros

entornos operativos fuera del ciberespacio por medio de instrumentos cibernéticos (Nye, 2010, p.9).

Dentro del ciberespacio se debe recalcar que es posible producir poder duro por medio de ataques cibernéticos y blando por medio de instrumentos de información para establecer agendas, atraer y persuadir a otros actores. Tomando el caso de estudio entre WikiLeaks y EE. UU que es un país con impresionantes recursos tanto de poder duro y blando, en la siguiente tabla[8] se va a poder ilustrar los tipos de poder por medio de las acciones emprendidas por Estados Unidos frente al caso de WikiLeaks, teniendo en consideración los tres aspectos o capas del poder en el nuevo dominio el ciberespacio.

*Tabla 3.2 Capas del poder en el ciberespacio*

| Tres Capas del Poder en el ciberespacio |
|---|
| 1era Capa: **La habilidad que tiene un actor para hacer que los otros hagan lo contrario a sus preferencias iniciales**<br><br>• **Acciones de Poder Duro:**<br>Tras las filtraciones WikiLeaks sufrió ataques cibernéticos de denegación de servicio por parte de EE. UU.<br>Detención del soldado estadounidense Bradley Manning por filtrar información a WikiLeaks<br><br>• **Acciones de Poder Blando:**<br>Campaña "Stop, Think & Connect" para promover la conciencia del uso del ciberespacio lanzada en el 2010<br>Reclutamiento de hackers por medio de la Iniciativa Hackea al Pentágono 2012 |
| 2da Capa: **Establecer Agenda es la habilidad que tiene un actor para evitar las elecciones de otro al excluir sus estrategias. Si esto va en contra de su voluntad, es un aspecto del poder duro; si se acepta como legítimo, es considerado poder blando.**<br><br>• **Acciones de Poder Duro:**<br>Ejercer presión para que diferentes empresas que prestaban servicios a WikiLeaks quiten su apoyo para que la página web desaparezca. |

[8] La tabla ha sido realizada en base a los ejemplos y características para observar al poder dentro del ciberespacio, la que ha sido creada por Nye en su obra "Cyberpower". Ver tabla 2 (Nye, 2010, p.7)

| |
|---|
| • **Acciones de Poder Blando:**<br>El 3 de diciembre del 2010 se reforma la Ley de Espionaje que exprese que se prohíbe la publicación de información clasificada del Estado.<br>En septiembre del 2010 se ordenó realizar los ejercicios *Cyber Storm* III para fortalecer la preparación cibernética como una máxima prioridad para la seguridad nacional. Además, *Cyber Storm* fue el vehículo principal para ejercer el recién desarrollado Plan Nacional de Respuesta a Incidentes Cibernéticos (NCIRP) y sirvió para probar por primera vez al *National Cybersecurity and Communications Integration Center* (NCCIC) que es el centro encargado de la coordinación nacional de ciberseguridad inaugurado en octubre del 2009. |
| 3ra Capa: **Es la habilidad que tiene un actor para moldear las preferencias iniciales del otro para que algunas estrategias nunca sean consideradas**<br><br>• **Acciones de Poder Duro:**<br>Persecución y amenazas contra Julian Assange "nombrarlo como un terrorista de alta tecnología" y pedir su muerte, acciones para eliminar a WikiLeaks<br><br>• **Acciones de Poder Blando:**<br>Inversión en Startups de ciberseguridad<br>Formar hackers éticos con altos estándares de moral por medio de la Iniciativa Nacional para la Educación sobre Ciberseguridad (NICE)<br>Proyecto *Cyber Insider Threat* para evitar traición de las personas que tienen acceso a las redes de información del Estado. |

Fuente: Cyber power, Nye (2010)
Elaborado por: Torres. P, 2020

Esta tabla sirve para ilustrar mejor como se emplea el poder en el ciberespacio e identificar las estrategias de poder blando y duro que los Estados Unidos utilizó sobre el caso de WikiLeaks, para intentar que la organización desapareciera y de esa manera evitar que siga amenazando y atentando a los intereses estadounidenses, es por eso, que estas acciones represivas en contra de WikiLeaks son una muestra común de ejercer poder para así evitar que diferentes actores pueden interferir en la distribución del poder (Armstrong, 2015, p. 36).

Entre acciones represivas también constan la creación y uso de las leyes para ser utilizadas como un instrumento político "para contrarrestar, suprimir y vigilar las actividades que están etiquetadas como socialmente desviadas" (Armstrong, 2015, p. 36). Es decir, las leyes son específicamente creadas con el fin de crear orden social para

que el Estado pueda expresar su poder imponiendo lo que es permitido hacer y por quién. Se puede decir que las leyes son un tipo de manipulación que ejerce el Estado para controlar a las disidencias que puedan emerger (Armstrong, 2015, p. 37).

## 3.2 Inversión en capacidades cibernéticas para mejorar la ciberseguridad de los Estados Unidos

El gasto de los Estados Unidos en operaciones cibernéticas e inteligencia se compone por dos programas con propios presupuestos, por una parte el Programa de Inteligencia Nacional (NIP) que se encarga del apoyo estratégico, creación de políticas y manejo de los programas, proyectos y actividades de la comunidad de inteligencia orientada a abastecer las necesidades estratégicas de los tomadores de decisiones y por otra, el Programa de Inteligencia Militar (MIP) que se encarga del financiamiento de la inteligencia para operaciones de defensa como brindar apoyo operativo y táctico (De Vine, 2019, p. 5).

Para Estados Unidos es fundamental incrementar el presupuesto que está destinado a acional contaba con un presupuesto de 47 000 millones de dólares, pero este valor ha venido aumentando por encima del incremento del PIB del país (Pastor, Pérez, Arnáiz de la Torre, & Toboso, 2009, p. 70). Desde el 2008 ha aumentado entre el 8 al 9%. Pero específicamente para el área de ciberseguridad según los analistas indicaron que el presupuesto superaría a los 10 000 millones de dólares hasta el final de la administración de Barack Obama (Pastor, Pérez, Arnáiz de la Torre, & Toboso, 2009, p. 70).

Para el 2013 estuvo prospectado que el presupuesto para la seguridad de las redes militares de inteligencia de las agencias se incremente un 44 % más, lo que llegaría a ser más de 10 700 millones de dólares (Pastor, Pérez, Arnáiz de la Torre, & Toboso, 2009, p. 70). Es un hecho que desde la década pasada era imprescindible incrementar cada año

el presupuesto en materia de ciberseguridad y operaciones cibernéticas, lo que muestra que la dependencia en el ciberespacio cada vez se intensifica más. Por ejemplo, en marzo del 2019 Director de Inteligencia Nacional anunció que solicitaría la suma más grande de la historia de 62 800 millones de dólares para el 2020 (Swab, 2019, p.4)

Dentro del presupuesto del NIP abarca 17 agencias que forman parte de la comunidad de inteligencia estadounidense, el presupuesto del MIP financia programas de la Agencia de Inteligencia de Defensa (DIA) la Agencia Nacional de Inteligencia Geoespacial (NGA), la Agencia de Seguridad Nacional (NSA), entre otros. Además, los fondos del MIP están también dirigidos para el Ejército, la Armada, la Fuerza Aérea y la Marina brindando apoyo a cada una de las actividades de inteligencia en estos servicios (Swab, 2019, p.7).

En la siguiente tabla se puede ver el aumento de los gastos de Inteligencia Nacional que incluye a ambos programas NIP y MIP desde el 2008 al 2020. Esta tabla ilustra la magnitud del incremento de los montos en inteligencia que reflejan la importancia para los Estados Unidos para mantener y salvaguardar la seguridad nacional en el ciberespacio.

*Tabla 3.3 Gastos de Inteligencia de EE. UU del 2008 al 2019*

| **Gastos de Inteligencia del 2008 al 2019<br>Dólares en miles de millones, redondeados** | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 2007 | 2008 | 2009 | 2010 | 2011 | 2012 | 2013 | 2014 | 2015 | 2016 | 2017 | 2018 | 2019 |
| **NIP** | 43.5 | 47.5 | 49.8 | 53.1 | 54.6 | 53.6 | 52.7 | 50.5 | 50.3 | 53.0 | 54.6 | 59.4 | 60.2 |
| **MIP** | 20.0 | 22.9 | 26.4 | 27.0 | 24.0 | 21.5 | 19.2 | 17.4 | 16.5 | 17.7 | 18.4 | 22.1 | 21.2 |
| **TOTAL** | 63.5 | 70.4 | 76.2 | 80.1 | 78.6 | 75.4 | 67.6 | 67.9 | 66.8 | 70.7 | 73.0 | 81.5 | 81.4 |

Fuente: Congressional Research service, 2019
Elaborado por: Torres, P. 2020

Por otra parte, para el Pentágono las amenazas cibernéticas han causado preocupación ya que, anunciaron que de acuerdo a los nuevos lineamientos de la administración de Obama para aumentar la protección de las redes informáticas han adquirido un nuevo comando digital, para cumplir con las metas establecidas por la nueva administración (Pastor, Pérez, Arnáiz de la Torre, & Toboso, 2009, p. 76). El ejército creó una nueva unidad operativa con el nombre de cibercomando que se dedica exclusivamente a realizar acciones de ataque y defensa en el ciberespacio (Pastor, Pérez, Arnáiz de la Torre, & Toboso, 2009, p. 70).

Además, los resultados del examen de control a ordenadores de las agencias de inteligencia y seguridad dieron que el 70% de estos no tenían la codificación adecuada para resistir a ataques externos, lo cual, era una alerta sobre las fallas de seguridad que EE. UU enfrentaba, es por eso, que el Pentágono gastó 74 millones de dólares aproximadamente para responder a ataques y reparar daños que provocaron estas fallas de seguridad (Pastor, Pérez, Arnáiz de la Torre, & Toboso, 2009, p. 72).

No se debe pasar por alto lo reciente que es el ciberespacio, Estados Unidos que es uno de los países pioneros en iniciativas para este dominio, solo empezó la década pasada a desarrollar sus primeros planes serios para el ámbito de la ciberseguridad. Este factor de ser un fenómeno muy reciente, pero con gran importancia y alta dependencia causa que mientras los países están desarrollando iniciativas, planes, programas y políticas para estar más seguros, por otro lado, también se vuelven vulnerables a diferentes tipos de ataques y desafíos que están recién descubriendo (Nardoianni, 2016, p. 49).

También de esta necesidad de descubrir alternativas para estar protegido en el ciberespacio nace el término de la ciberpolítica, que se refiere a la fusión de dos procesos. Por un lado, están las que se relacionan con las interacciones humanas

(políticas) y, por otro, las que están habilitadas por el uso del espacio virtual (ciber) como un nuevo escenario que tiene sus propias modalidades y realidades (Choucri, 2013, p. 4).

El compromiso de la administración de Obama con la ciberseguridad es imparable ya que, por medio del desarrollo de diferentes tipos de iniciativas se van a ver los efectos positivos de aumentar sustancialmente las capacidades cibernéticas (Nardoianni, 2016, p. 103). La inversión en ciberseguridad es un factor primordial en la política estadounidense, la administración de Obama se propuso en otorgar un fondo de 3,1 mil millones de dólares para modernizar la tecnología de la información y para aumentar la seguridad creó un nuevo cargo de Director Federal de Seguridad de la Información, con el objetivo de impulsar cambios notables en términos de seguridad cibernética en todo el Gobierno (Nardoianni, 2016, p. 103).

### 3.3 El rol de las agencias implementadas por los Estados Unidos para afrontar amenazas cibernéticas, reducir la vulnerabilidad, aumentar sus capacidades y poder en el ciberespacio.

La importancia de entender el nuevo contexto internacional del que emerge el ciberespacio conlleva a que se fomente la colaboración entre los actores gubernamentales que trabajan persiguiendo el interés común de mantener la seguridad del Estado mediante la implementación de ciber-gobernanza que se encarga de abordar temas de creación de instituciones para la gestión y seguridad cibernética. Es por esto, que es de vital relevancia lograr el funcionamiento efectivo de las interacciones en el ciberespacio a través de la efectividad de las instituciones destinadas para gestionar el ciberespacio (Choucri, 2013. P. 162).

Estados Unidos cumple un papel fundamental en el liderazgo de implementación de ciber-gobernanza, desde el principio de la expansión del uso del internet han ido

reconociendo que las vulnerabilidades cibernéticas son una realidad que trae peligro no solo a la seguridad de la información en las redes del gobierno, sino también, a la seguridad de los ciudadanos que día a día hacen uso de esta herramienta (Choucri, 2013. P. 163). Sin embargo, a raíz de incidentes cibernéticos que han mostrado las vulnerabilidades en ciberseguridad han hecho que los Estados Unidos esté consciente del impacto potencial de estas amenazas e incremente la gobernanza cibernética.

Las motivaciones y esfuerzos para fomentar la gobernanza del ciberespacio se iniciaron en la década de los noventa, es por eso que, a lo largo de los últimos años se ha visto la necesidad de crear agencias para fortalecer las acciones de respuesta frente a las amenazas y desafíos cibernéticos. Además, se debe tomar en cuenta la complejidad de la ciberseguridad de los Estados Unidos ya que, cuenta con demasiadas agencias que contienen gran variedad de programas de inteligencia y seguridad. Es por eso, que se ha seleccionado a las agencias que tienen mayor relevancia para entender cómo se maneja la ciberseguridad en los Estados Unidos. Principalmente, se debe mencionar a la Oficina del Director de Inteligencia Nacional (ODNI) que es la encargada de coordinar y de establecer objetivos de inteligencia de 17 agencias y organizaciones que están también bajo la responsabilidad de Departamento de Seguridad Nacional (DHS) y del Departamento de Defensa (DoD) (Nardoianni, 2016, p. 101).

Entre las agencias y centros principales de ciberseguridad de los Estados Unidos están la Agencia Nacional de Seguridad (NSA), Agencia de Seguridad Cibernética e Infraestructura (CISA) y una nueva agencia “Centro de Integración de Inteligencia de Amenazas Cibernéticas". La Agencia de Seguridad Nacional (NSA) que forma parte del Departamento de Defensa está en cargada de brindar servicios de inteligencia al gobierno estadounidense para defender las redes de vital importancia, por medio de su especialización en servicios de criptología e investigación, que es empleada para

descubrir secretos de adversarios y proteger la información secreta de los EE. UU de esta manera superar a las amenazas del ciberespacio (NSA, 2018).

La Agencia de Seguridad Cibernética e Infraestructura (CISA), surgió en el 2007 bajo una iniciativa de la Subsecretaría de Seguridad Nacional para Protección Nacional y Programas y tenía el nombre de Dirección Nacional de Protección y Programas (NPPD), pero, no fue hasta el 2018 que fue creada oficialmente como agencia bajo la ley y fue firmada por el nuevo presidente Donald Trump (CISA,2018). Esta agencia terminó reemplazando a la antigua NPPD que cumplía con la función principal de proteger la infraestructura física y cibernética crítica de la nación y los recursos clave contra de diferentes tipos de ataques terroristas, entre otros incidentes graves (CISA, 2018). Es decir, el rol de la NPPD era de gran importancia ya que, contenía al Centro de Integración de la Ciberseguridad Nacional y Comunicaciones (NCCIC) que fue creado en octubre del 2009, con la finalidad de reducir el riesgo de desafíos sistémicos de ciberseguridad enfocado en dar servicios de defensa cibernética, análisis y dar respuestas ante los incidentes cibernéticos. Por otra parte, también contenía a la U.S – CERT que es la entidad encargada de la defensa de las redes federales y civiles, proteger el proceso de compartir información y colaborar con otras entidades del sector privado en temas de ciberseguridad (Choucri, 2013, p. 167)

Desde su reciente creación es la institución que tiene la función de ser el asesor de riesgos de EE. UU, debido a que proporciona amplio conocimiento y prácticas de ciberseguridad de infraestructuras tecnológicas, para que la nación pueda mitigar todo tipo de amenazas y vulnerabilidades (CISA, 2018). Entre sus principales funciones se encarga de garantizar la protección de la red federal y de la cibernética de todo el país, intercambiar información cibernética, mejorar las comunicaciones

del gobierno federal, desarrollar capacidades para el uso de comunicaciones de emergencia, asegurar la resiliencia de la infraestructura y operaciones de campo, se ocupa de la generación de respuestas y del proceso de recuperación frente a incidentes significativos dentro y fuera del gobierno (CISA, 2018).

Por último, tenemos a la nueva agencia del gobierno federal "Centro de Integración de Inteligencia de Amenazas Cibernéticas" que surgió por iniciativa de la Oficina del Director de Inteligencia Nacional (ODNI) en el 2015 en manera de implementar las lecciones aprendidas durante estos años combatiendo acciones terroristas en el ciberespacio (CTIIC, 2015). Este centro integra inteligencia sobre las amenazas extranjeras que pueden surgir que dañan a los intereses del país, por lo que, es importante que forme parte del Centro Nacional de Integración de Ciberseguridad y Comunicaciones (NCCIC), la Fuerza de Tarea Conjunta Nacional de Investigación Cibernética (NCIJTF) y el Comando Cibernético de los Estados Unidos para proteger a la nación de las ciberamenazas (CTIIC, 2015).

El CTIIC tiene seis responsabilidades fundamentales. Se encarga de garantizar que la información se comparta entre la comunidad cibernética federal, realizar análisis integrados de las amenazas cibernéticas, apoyar la gestión de los analistas y formuladores de políticas de inteligencia, supervisa el desarrollo y la implementación de capacidades de intercambio de inteligencia, asegurar que los indicadores de actividad cibernética maliciosa se mantengan lo más bajo y facilitar y apoyar los esfuerzos interinstitucionales para desarrollar e implementar planes coordinados para contrarrestar las amenazas cibernéticas extranjeras por medio de todos los instrumentos del poder nacional posibles lo que también incluye a las actividades diplomáticas, económicas, militares, y de aplicación de la ley (CTIIC, 2015).

Estas agencias mencionadas tienen los roles principales para hacer frente a las amenazas cibernéticas, reducir las vulnerabilidades, dar respuesta a los incidentes para poder resolver problemas y mitigar daños que pueden tener graves consecuencias a la seguridad nacional del país. El trabajo de estas agencias tiene el objetivo de aumentar capacidades cibernéticas para contrarrestar peligros y, por lo tanto, también aumentar el poder y el control en el ciberespacio. El desarrollo y creación de políticas y agencias de ciberseguridad en los EE. UU se ha podido ver que especialmente desde la administración de Obama han tomado más fuerza e importancia.

Por eso, para el desarrollo de esta investigación que se basa en identificar la posible influencia de la organización WikiLeaks en la formación de políticas y agencias de ciberseguridad. Se debe comenzar con la asociación de los hechos entre las revelaciones de WikiLeaks y las acciones que tomó el gobierno estadounidense en temas de aumentar la ciberseguridad en la nación las cuales han sido descritas a lo largo de este capítulo y en el capítulo anterior.

Además, se debe recalcar que la identificación de la participación de WikiLeaks por medio de sus acciones anti-hegemónicas como la "filtración de información" es relevante, ya que, esto sirvió para impulsar y fomentar aún más la creación de políticas y agencias de seguridad en EE. UU. Esta intuición sobre las posibles repercusiones de WikiLeaks que se han formado y creado a lo largo del proceso de esta investigación busca ayudar a entender y reconocer el rol y la relevancia de actores no estatales con las características de WikiLeaks para poder operar en el ciberespacio, en donde, es posible el empoderamiento de actores que buscan alcanzar un protagonismo alterando al sistema internacional convencional. Para continuar con el análisis sobre la incidencia del accionar de esta organización a continuación se ha propuesto una tabla en donde se relaciona las acciones de WikiLeaks con las acciones de respuesta del gobierno

estadounidense para aumentar sus capacidades de respuesta y de defensa frente a las amenazas cibernéticas que ponen en riesgo a su seguridad. Sin embargo, se debe tomar en cuenta que hasta esta época ya existían otras amenazas en el ciberespacio por parte de otros actores que no eran WikiLeaks, pero también, el caso con WikiLeaks ha sido uno de los que más sonados por el impacto mediático que obtuvo y porque desde sus inicios antes del 2010 ya había filtrado información sobre el gobierno estadounidense.

*Tabla 3.4 Relación de las acciones de WikiLeaks con las políticas y planes implementados en respuesta por parte del gobierno estadounidense frente a las acciones de WikiLeaks tras las filtraciones*

| ACCIONES ANTIHEGEMÓNICAS DE WIKILEAKS | POLÍTICAS E INICIATIVAS POR PARTE DEL GOBIERNO DE EE.UU EN RESPUESTA |
|---|---|
| En 2006 WikiLeaks inició sus operaciones hasta el 2009 la organización ya había publicado sus primeras filtraciones masivas de información confidencial sobre el gobierno estadounidense. | • En 2009 Obama inició su mandato ordenando una Revisión de todas las iniciativas federales en ciberseguridad.<br>• Pidió al Consejo de Seguridad Nacional que desarrolle un enfoque global sobre ciberseguridad.<br>• Creó por primera vez el cargo de coordinador de ciberseguridad con la finalidad de que trabaje directamente en asesorar al presidente en temas de ciberseguridad y asesore la creación de nuevas políticas.<br>• Nombró a la ciberseguridad como un tema de "prioridad nacional" y declaró a la infraestructura digital como un activo estratégico nacional. |
| Filtraciones en el 2010:<br>*Collateral Murder*<br>Los diarios de guerra de Afganistán<br>Papeles de la guerra de Iraq<br>*Cablegate* | • Estas publicaciones impulsaron a la creación de política de control de daños según fueron las declaraciones de la secretaria de Estado Hillary Clinton frente a las publicaciones de WikiLeaks poco después el gobierno publicó el "Plan Nacional de Respuesta a los Incidentes Cibernéticos.<br>• 2010 Obama presenta su Primera Estrategia de Seguridad Nacional, la cual es la primera estrategia que señala y resalta al ciberespacio como una amenaza. |

| | |
|---|---|
| | • En 2010 a pocos días de la última publicación de WikiLeaks *Cablegate*, se creó el cargo de Asesor Principal del Personal de Seguridad Nacional para el acceso a información y política de Seguridad.<br>• 2010 Lanzó Campañas para promover la concientización del uso del ciberespacio, debido a que las filtraciones fueron de gran repercusión mediática lo que ha motivado a generar sensibilidad ciudadana sobre el ciberespacio.<br>• En 2011 se firmó la Orden Ejecutiva 13587 para mejorar la seguridad de las redes clasificadas y el intercambio responsable y la salvaguarda de la información clasificada<br>• 2011 Estrategia Internacional para el ciberespacio |

Elaborado: Torres. P, 2020

Después de las revelaciones de WikiLeaks, los departamentos con sus respectivas agencias gubernamentales se enfocaron en revisar su uso de bases de datos clasificadas y comenzaron a implementar varias medidas que principalmente se relacionaban con el compartimiento de información entre las agencias (Fenster, 2012, p. 790). El secretario de defensa Robert Gates ordenó dos revisiones de la seguridad de los documentos e información y realizó evaluaciones para ver la vulnerabilidad de las redes del DOD para mejorar la concientización de cumplir con los nuevos procedimientos de protección de información que fueron más estrictos y contaron con la implementación de más tecnología para evitar que estos hechos vuelvan a suceder (Garamore, 2010).

*Tabla 3.5 Relación de las acciones de WikiLeaks con las Agencias de ciberseguridad y sus iniciativas creadas por el gobierno estadounidense*

| **Accionar de WikiLeaks** | **Iniciativas del gobierno de Obama Rol con las agencias de ciberseguridad** |
|---|---|
| | La Oficina del Director Nacional de Inteligencia ODNI se encarga |

| | |
|---|---|
| Las filtraciones de información confidencial sobre el gobierno estadounidense | específicamente en mejorar el intercambio de información con todas las agencias, es por eso que WikiLeaks impulsó indirectamente a que la ODNI trabaje en las mejoras del manejo de información en todo el gobierno. |
| | Creación del Centro de Integración de Inteligencia de Amenazas Cibernéticas 2015, esta agencia es creada por la necesidad de incrementar sus capacidades frente a las amenazas de piratas informáticos como WikiLeaks y otros atacantes a los sistemas de información estadounidenses. |
| | Creación del cargo de Director Federal de Seguridad de la Información con el rol de crear nuevas políticas de seguridad para todas las agencias para evitar que EE. UU sea vulnerable a un ataque o robo de información. |
| La mayor parte de los documentos publicados fueron robados por Brandley Manning un soldado estadounidense que logró tener acceso a las redes y robar la información que fue entregada a WikiLeaks | A raíz del caso con Manning el Departamento de Defensa por medio de su Agencia DARPA "Agencia de Proyectos de Investigación Avanzados de Defensa", creó el programa "*The Cyber Insider Threat*" para detectar amenazas internas que puedan robar información no autorizada. |

Elaborado: Torres, P. 2020

A lo largo de este capítulo se puso en discusión sobre el avance tecnológico y la evolución del internet que han creado un espacio virtual en donde la participación de distintos tipos de actores ha causado muchos desafíos a los Estados. Es por eso, que la importancia que tiene del ciberespacio en la actualidad abre un extenso debate sobre como los Estados que siguen siendo los actores principales se tienen que organizar para ganar poder y gobernanza dentro de este nuevo dominio, que indudablemente tiene incidencias políticas, gracias, a la alta dependencia del Estado y de los individuos al ciberespacio. En donde surgen muchas oportunidades para que los actores con mínimos recursos puedan causar disrupción en el orden internacional

y amenazar a las estructuras de poder establecidas. Durante el capítulo también sobresale que la época actual está dominada por el uso de tecnologías que siempre están evolucionando, estos avances también llegan a tener una incidencia en el poder que se encuentra en constante transición y difusión, y ya no solo, se basa en la posesión de recursos materiales, sino que más bien el poder se está volviendo menos tangible dentro del contexto en el que se encuentra.

El poder en el ciberespacio se encuentra fusionado por el uso de estrategias de poder blando y duro, pero, lo preocupante es que no solo los Estados pueden hacer uso de estas estrategias el mayor peligro es que debido a los bajos costos para entrar al ciberespacio los pequeños actores tienen capacidad de ejercer estrategias de poder en el ciberespacio. Lo que significa, que en el ciberespacio las posibilidades de ejercer control total sobre este dominio para los grandes y poderosos actores estatales se reduce, lo que termina causando preocupación para incrementar capacidades cibernéticas para estar seguros en el ciberespacio.

Como en el caso de Estados Unidos que por los sucesos con WikiLeaks logró mostrar las vulnerabilidades, debilidades y fallas de ciberseguridad. No obstante, es uno de los países que ha liderado y lidera en iniciativas, políticas, estrategias, tecnología e innovación. Esto demuestra el compromiso que tiene para llegar a ganar el poder y salvaguardar sus intereses y la seguridad nacional en el quito dominio. Es por eso, que en este capítulo se logró reconocer la relevancia de WikiLeaks como un actor transnacional en el ciberespacio que por el uso de la información y herramientas cibernéticas influyó directa e indirectamente en que EE. UU refuerce sus capacidades para operar en el ciberespacio.

## VI. ANÁLISIS

Durante el transcurso de esta investigación que ha venido siendo guiada por el objetivo principal, el cuál trata en identificar si existe influencia por parte de WikiLeaks y sus filtraciones en la formación de políticas y agencias de ciberseguridad en los Estados Unidos. Primeramente, se debe tomar en cuenta que la revolución de la información que se ha implementado gracias al desarrollo tecnológico por la globalización ha impulsado a que el internet se convierta en una herramienta esencial para que se de esta revolución de tipo tecnológica en el ciberespacio. El papel principal y la gran importancia que ha logrado obtener el ciberespacio a lo largo de estas dos últimas décadas era inimaginable años atrás en sus inicios. Este es un lugar virtual de interacción abierta entre diferentes tipos de individuos que poseen diferentes características y habilidades, lo cual, lo convierte en un lugar no convencional en donde emergen distintas amenazas que con la ayuda del desarrollo tecnológico se vuelven cada vez más sofisticadas.

Retomando a los Estados Unidos como actor principal para el desarrollo de esta investigación se ha podido identificar que es un país que también desde los inicios del año 2000 ha identificado la importancia de enfocar su política exterior en torno al ciberespacio, por lo tanto, es una de las naciones pioneras que ha creado un complejo conjunto de normas, políticas y agencias para poder manejar los desafíos en el tema de ciberseguridad. A lo largo de los años el compromiso en protegerse en este nuevo dominio se ha consolidado fuertemente entre los temas principales de la agenda política. Por ejemplo, desde la administración de George W. Bush se impulsó la primera iniciativa para el ciberespacio en 2003 que la llamó *National Strategy to Secure Cyberespace*, la cual definió al ciberespacio como el sistema nervioso que controla los sistemas del país ya que, está compuesto por cientos de computadoras interconectadas a

servidores, enrutadores, interruptores y cables de fibras ópticas que permiten que la infraestructura critica del país funcione (Kuehl, 2009, p.2). Entre otra iniciativa de esa administración fue *Comprehensive National Cybersecurity Initiative* (CNCI) que fue retomada y rediseñada por la nueva administración de Obama (CNCI, 2010). Por consiguiente, para proseguir con el análisis que fue desarrollado en los capítulos anteriores, es notable que desde el inicio del período de Barack Obama en la presidencia de los EE. UU, esta fue la administración que le dio más énfasis a la importancia del ciberespacio y sobre todo a las acciones de ciberseguridad que debían ser implementadas para afrontar los desafíos cibernéticos, los cuales, ya estaban aumentando el nivel de preocupación y consciencia para esta nueva administración que sabía que no se encontraba lo suficientemente preparada como debía estarlo. Es por esto, que se ordenó una revisión exhaustiva a la política del ciberespacio para encontrar deficiencias, mejorar las normas sobre la seguridad de las infraestructuras críticas del Estado, reducir ciberamenazas y resistir ante los ataques cibernéticos de cualquier tipo.

Sin embargo, durante los primeros años de esta nueva administración sucedieron hechos que pusieron en alarma a los Estados Unidos. La aparición de WikiLeaks y sus filtraciones masivas de información confidencial sobre el gobierno estadounidense desató controversia, en torno a que se decía que estas tendrían un efecto perjudicial directo en la diplomacia, en la imagen, reputación, y por su puesto en la seguridad nacional del país (Packer, 2010). Pero, se debe decir que no existen las pruebas suficientes para constatar estos supuestos "efectos devastadores" de las filtraciones en el poder y la diplomacia estadounidense (Landler, 2011). Además, poco después de las filtraciones funcionarios del gobierno en sus declaraciones expresaron que los efectos que iban a tener de estas divulgaciones de información iban a ser mínimos en las

relaciones internacionales de los Estados Unidos y, por lo tanto, la imagen y la reputación de la nación se encontraban sin repercusiones graves (López, 2012, p. 81).

Por otra parte, las filtraciones si sirvieron para mostrar las fallas y errores cibernéticos, lo que aumentó la consciencia del gobierno sobre la importancia de incrementar y generar medidas efectivas de ciberseguridad. Aunque, la organización WikiLeaks buscaba con sus acciones generar impacto político en sentido de fomentar la transparencia de las acciones del gobierno para impulsar una mejor gobernanza internacional que ampare acciones responsables para proteger los derechos humanos e impulsar el progreso de sociedades sin corrupción. Sin embargo, la organización no logró alcanzar este ideal por el cual habían trabajado, sino que, el impacto fue a corto plazo ya que, durante el 2010 y el 2011 WikiLeaks con sus filtraciones solo logró fama internacional.

Durante ese período también su accionar ocasionó presión e impacto mediático y político para los funcionarios del gobierno de los principales departamentos encargados de velar por la seguridad nacional, pero, en sentido de elaborar e impulsar rápidas respuestas con políticas nacionales sobre asegurar el acceso a la información sensible e implementar más políticas de ciberseguridad dirigidas a corregir errores, mitigar efectos y recomendar nuevas estrategias, iniciativas y políticas entre todo el gobierno para fortalecer a los Estados Unidos en el ciberespacio frente a las publicaciones de WikiLeaks.

Es decir, en lo desarrollado en el primer capítulo se identificó parcialmente la injerencia de WikiLeaks en la fomentación de reformas en políticas y creación de iniciativas de ciberseguridad, debido a que, desde antes de que la organización se vuelva famosa por la revelación de información confidencial a gran escala sobre los EE. UU, la administración de Obama ya había empezado a realizar esfuerzos, debido a que, como

lo había pronunciado durante su campaña presidencial esta nueva gobernación estaba consciente de que el país no se encontraba lo suficientemente preparado para actuar en el ciberespacio y la actuación de WikiLeaks ayudó a demostrar las debilidades en ciberseguridad que el país tenía.

La respuesta de la administración de Obama desde la filtración de información fue agresiva frente a la organización, pero también, la filtración de millones de documentos de EE. UU incrementó la importancia del tema de ciberseguridad que fue reflejada, a través, de las cinco estrategias implementadas desde el 2010 especialmente durante el 2011 que fue el año con siete iniciativas creadas por primera vez por diferentes departamentos dirigidas para operar con seguridad en el ciberespacio, estas impulsaron y sirvieron como base para  más estrategias en los años posteriores (Conde, 2014). El empoderamiento de nuevos actores en el ciberespacio alertó sobre el desafío transnacional que esto significa y, por lo tanto, surgió la necesidad de crear planes y estrategias conjuntas para luchar contra estas amenazas de alcance global que no solo afectan a EE. UU.

Es por eso, que durante el desarrollo del segundo capítulo se puede ver que la respuesta del gobierno de Obama fue politizar a la ciberseguridad tanto como a nivel nacional e internacional. Entre las principales acciones que implementó por medio de sus planes que fueron enfocados en la necesidad de fomentar la cooperación internacional, de igual manera, EE. UU con su papel de liderazgo en el mundo, impulsó a que la ONU también fomente iniciativas con objetivos similares a los que EE. UU había planteado en sus planes anteriormente presentados, para que, tengan mayor alcance en la comunidad internacional que logré unir fuerzas e incrementar capacidades cibernéticas, y de esta manera  la seguridad nacional, los intereses económicos y políticos no vuelvan a caer en vulnerabilidad.

La relevancia y la dependencia al ciberespacio no solo ha venido creciendo para los usuarios de internet de todo el mundo, sino que, los Estados cada vez más son altamente dependientes, debido a que, es de vital importancia para lograr fines especialmente orientados al crecimiento económico, tecnológico y de seguridad. Por lo cual, el ciberespacio es conocido como el nuevo quinto dominio y emerge el desafío de llegar a controlar este espacio que posee características muy diferentes a los otros dominios existentes. Dentro de este nuevo dominio coexisten actores estatales y diferentes tipos de actores no estatales, lo que causa, que el poder este en constante cambio, debido a, que las barreras de entrada son mínimas, los costos son baratos, lo que motiva a que estos actores puedan ganar poder para lograr actuar maliciosamente por medio del uso de tecnologías.

En el desarrollo del tercer capítulo se puede ver el papel que tienen los actores no estatales especialmente el de WikiLeaks como un actor transnacional con características diferentes a los otros actores ya que, utilizó a la información como una herramienta de poder dentro de este dominio para intentar afectar a la hegemonía estadounidense y causar disrupción en el orden internacional. Es por eso, que el accionar de estos actores influye, porque han logrado replantear la naturaleza del poder que dentro de este dominio y en este contexto este poder depende de la combinación de acciones de *hard and soft power* con el uso de recursos tecnológicos. Esto según, el autor Joseph Nye le atribuyó el nombre de ciberpoder (Nye, 2010, p. 3).

En este capítulo se pudo reconocer la importancia de las amenazas que representan los actores transnacionales como WikiLeaks, que, en este caso, por medio de sus acciones anti hegemónicas mostró fallas y las debilidades de ciberseguridad de los Estados Unidos, además, en este caso se notó las habilidades que posee esta nación para hacer uso de estrategias de defensa basadas en poder blando y duro para afrontar

las consecuencias de las filtraciones a su seguridad nacional. Es por eso, que como parte de la estrategia de poder duro EE. UU vio la necesidad de trabajar exhaustivamente para incrementar y reforzar sus capacidades cibernéticas para evitar que este tipo de actores vuelvan a atacar sus sistemas de información sensibles y de igual manera, el aumento de capacidades cibernéticas sirve para ganar poder en este nuevo dominio y que sea capaz de proteger los intereses nacionales y salvaguardar la seguridad nacional dentro del ciberespacio que es relativamente nuevo. Lo que significa, que para estar seguros deben estar preparados tecnológicamente, para así, poder estar en permanente lucha con diferentes actores que tienen las posibilidades de alcanzar las mismas capacidades.

Para identificar mejor el cumplimiento de la hipótesis de esta disertación que propuso que la organización transnacional WikiLeaks, por medio de sus acciones anti hegemónicas en el ciberespacio, provocó la creación de políticas y agencias de ciberseguridad que fortalecieron a la hegemonía estadounidense en el período 2010-2015. Se debe decir que el análisis de esta investigación se resolvió con una metodología mixta que permitió combinar datos cualitativos y cuantitativos para poder observar las realidades objetivas y subjetivas que plantea el problema de esta disertación. Las técnicas seleccionadas para realizar la presente investigación fueron: descripción de indicadores, observación, entrevistas, recolección de datos escritos, numéricos y documentos.

Además, se utilizó específicamente el método de análisis de contenido acorde al manual de investigación cualitativa de Saldaña (2013) ya que, es una técnica que pertenece a las medidas o formas discretas de investigación, debido, a que se encarga de estudiar los comportamientos sociales sin que estos se vean afectados (Babbie, 1975, p. 295). Es por eso, que esta técnica facilitó el análisis gracias a que permite examinar artefactos sociales como los documentos escritos, discursos políticos, leyes, contenido

de sitios web, libros, es decir, el análisis de contenido es el estudio de las comunicaciones de los seres humanos que son grabadas de diferentes maneras (Babbie, 1975, p. 296). Sin embargo, se debe mencionar que este método presenta limitaciones en cuanto a la subjetividad para clasificar la información en diferentes categorías, fue una tarea difícil dada la abundancia y heterogeneidad del tema.

Para esta investigación se ha tomado como muestra a los discursos, entrevistas y publicaciones de los diferentes actores más relevantes de los departamentos del gobierno de Obama en torno a declaraciones sobre las filtraciones de WikiLeaks, además, para que la muestra sea representativa se ha seleccionado documentos publicados, entrevistas, declaraciones sobre las iniciativas, estrategias y políticas de ciberseguridad más relevantes que fueron implementadas poco después de las publicaciones de WikiLeaks. Los discursos y documentos seleccionados serán analizados por medio de codificación de información, ya que, la codificación es una operación esencial en el análisis de contenido, debido a que esta sirve para transformar la información simple a una forma estandarizada y se la puede clasificar de acuerdo con los marcos conceptuales y teóricos establecidos de la teoría de la interdependencia compleja con sus actualizaciones por el autor Joseph Nye.

La codificación utilizada para el análisis de contenido del presente trabajo fue la codificación manifiesta de materiales, debido a que, se caracteriza por ser objetiva y ayuda rápidamente a observar el contenido superficialmente visible, lo que quiere decir, que se distinguen los elementos más sobresalientes para ser contados (Babbie, 1975, p. 301). Por ejemplo, identificar las palabras que son más repetitivas para poder establecer un significado o un juzgamiento sobre los efectos de las acciones de WikiLeaks en la creación de políticas y estrategias de ciberseguridad en los Estados Unidos. Es por eso, que en cuanto a la parte cuantitativa del análisis esta se ha basado en establecer la

frecuencia valorativa (suma total de todas las expresiones encontradas), la frecuencia proporcional (porcentaje asignado de la frecuencia de cada código) y la distribución de las frecuencias (repartir la frecuencia total entre todas las categorías existentes) (Saldaña, 2013).

Por consiguiente, a lo largo de la investigación se ha recolectado y seleccionado 17 documentos oficiales del gobierno de EE. UU. Los cuales, están representados por hojas de trabajo del gobierno, discursos sobre ciberseguridad de Barack Obama, entrevistas, declaraciones y presentación de estrategias, planes de ciberseguridad dictados por diferentes funcionarios del gobierno estadounidense (Ver anexo: 133). Para realizar el proceso de codificación de los documentos, se ha identificado tres categorías para poder encontrar la posible influencia de la organización WikiLeaks en la formación de políticas y agencias de ciberseguridad que fortalecieron su hegemonía. Las tres categorías son: Fortalecimiento de la hegemonía, aumento de ciberseguridad y acciones anti hegemónicas de actores no estatales transnacionales y los peligros en el ciberespacio. Estas categorías fueron seleccionadas deductivamente, lo que quiere decir que son categorías que vienen del problema y son previamente establecidas ya que, se han construido en base de referentes teóricos y sobre lo que se ha dicho de WikiLeaks (Díaz, 2018, p. 1).

El proceso de codificación fue guiado por un libro de códigos en el cual se asociaron las categorías deductivas seleccionadas que se aplicaron a los documentos de análisis (Ver tabla 4.1: 111). En lo que respecta al formato de la elaboración y extracción de códigos, se elaboró tablas para cada unidad de análisis las cuales están divididas en tres columnas. La primera contiene el texto transcripto y se resaltó con negrilla las frases que hacen referencia a las diferentes categorías principales, la segunda columna se refiere a la extracción de códigos preliminares los cuales son notas

analíticas que van a ayudar a encontrar el código final, y la tercera columna es de los códigos finales (Ver anexo: 133). En total se analizó 169 expresiones que pertenecen a las tres categorías mencionadas anteriormente.

Para comenzar con la primera categoría se encontró un total de 20 expresiones que hacen referencia al fortalecimiento de la hegemonía de los EE. UU los códigos que sustentan esta categoría son: prestigio internacional, liderazgo en el ciberespacio, Ciberespacio nuevo dominio de poder y ciberpoder. Los resultados de las tablas de codificación mostraron que el código con más repeticiones fue ciberpoder con un total de 8 repeticiones, le sigue el liderazgo en el ciberespacio con 7 repeticiones, prestigio internacional con 4 repeticiones y, por último, ciberespacio nuevo dominio de poder con solo 1 repetición. En conclusión, esta categoría representa el 12% sobre el 100% para poder ver este resultado que muestra el porcentaje de la incidencia de la organización WikiLeaks en el fortalecimiento de la hegemonía de EE. UU (Ver tabla 4.2: 112).

No obstante, durante el análisis se puede encontrar que EE. UU en sus diferentes planes, estrategias resalta el papel de liderazgo que ha venido ejerciendo a lo largo de los años en el sistema internacional y destaca su importancia de extender este liderazgo en el ciberespacio ya que, es una nación que como creadora de lo que hoy se conoce como el Internet tiene la responsabilidad de garantizar la seguridad de los individuos en el ciberespacio, y aún más, con la constante evolución de amenazas cibernéticas lo que ha motivado a crear estrategias para persuadir a otros Estados sobre las medidas que se deben implementar en ciberseguridad para operar en el ciberespacio y ejercer un control para reducir los riesgos que traen las actuaciones de diferentes actores estatales como no estatales.

Además, resalta el rol de la importancia de la cooperación internacional como una estrategia para luchar contra las amenazas cibernéticas, pero también, por medio de

estas estrategias de fomentar e incentivar la cooperación estaba intentado persuadir a los otros Estados de que compartan su visión de orden mundial y acaten este liderazgo que en este caso es en el ciberespacio (Keohane,1984).

La segunda categoría que corresponde al aumento de ciberseguridad se encontraron en total 108 expresiones, estas fueron codificadas en esta categoría por su referencia específica a la prioridad y acciones del gobierno por incrementar medidas de ciberseguridad. Se ha podido ver que esta categoría de la hipótesis representa el mayor porcentaje entre las otras dos ya que, está representa al 64% sobre 100% (Ver tabla 4.2: 112). Entre los 20 códigos que sobresalen de esta categoría se encuentran los siguientes con mayor número de repetición a lo largo del análisis, los cuales son: Innovación tecnológica en ciberseguridad con 18 repeticiones, le sigue reformas y revisiones en políticas sobre protección y seguridad de infraestructuras críticas de información con 14 repeticiones; seguridad y protección de información con 10 repeticiones; políticas, estrategias, programas y leyes de ciberseguridad y proteger la seguridad nacional con 9 repeticiones y por último con 6 repeticiones especialistas en ciberseguridad para evaluar riesgos y amenazas cibernéticas (Ver tabla 4.3: 112).

Se puede ver que estas expresiones muestran la importancia que toma la ciberseguridad durante el gobierno de Barack Obama, al ser la categoría que tiene más códigos relacionados al aumento de la seguridad de la nación en el ciberespacio. Con el código de innovación tecnológica en ciberseguridad que obtuvo el mayor porcentaje de esta categoría con el 11% se infiere en como los EE. UU se enfocó en aumentar y mejorar sus capacidades cibernéticas, a partir, de los sucesos de WikiLeaks se vio la importancia de innovar más en tecnología para aumentar la seguridad de las infraestructuras tecnológicas, específicamente en el manejo de la información entre las

agencias y departamentos del gobierno en donde pueden existir vulnerabilidades en el proceso de manejar y controlar información clasificada.

Es por eso que, la organización WikiLeaks impulsó órdenes ejecutivas específicamente enfocadas en mejorar la seguridad de las redes clasificadas, el intercambio responsable y la protección de la información clasificada. Además, este código refleja la importancia de estar constantemente innovando en tecnología para estar un paso adelante que otras naciones o de actores no estatales, para que, de esta manera puedan prevenir ataques cibernéticos y con más innovación obtener mayor seguridad, más poder y estabilidad dentro de este dominio.

El segundo código más repetido de esta categoría con el 8%, es el que se refiere a las reformas y revisiones en políticas sobre protección y seguridad de infraestructuras críticas de información. En los documentos seleccionados que se refieren a los esfuerzos de mitigación del gobierno de EE. UU sobre la divulgación ilegal de información clasificada por WikiLeaks. Se encontró la importancia de estudiar y desarrollar nuevas reformas necesarias para evitar que estos hechos vuelvan a suceder. La filtración de información por la organización impulsó a la creación de un grupo de trabajo de expertos en el tema de ciberseguridad para hacer revisiones exhaustivas a los procesos de manejo y almacenamiento de información confidencial de todo el gobierno, y también, para establecer medidas para mitigar los efectos que produjeron las acciones de WikiLeaks.

Por otra parte, las reformas y revisiones en políticas sobre protección y seguridad de infraestructuras críticas de información, también, fueron impulsadas desde el inicio del mandato de Obama, el cual pocos meses después de estar en el cargo de Presidente en el 2009 ordenó una revisión general del estado de ciberseguridad del país, está revisión impulsó iniciativas y reformas que generaron otras estrategias en este

ámbito que fueron ya mencionadas durante el desarrollo de los capítulos anteriores. Sin embargo, no se puede desligar las actuaciones de WikiLeaks ya que, los sucesos del 2010 incidieron en la politización de la ciberseguridad la cual llegó a ser un tema principal en la agenda política de los EE. UU durante el 2010 y el 2011.

En los años posteriores a las revelaciones se siguió impulsando acciones para continuar con la misión de cuidar a la nación en el ciberespacio, pero, se debe resaltar que durante el 2010 y 2011 se crearon más estrategias y planes de ciberseguridad para salvaguardar las infraestructuras críticas de información, aumentar acciones de respuestas y de defensa a las amenazas cibernéticas que en los años posteriores a las filtraciones de WikiLeaks.

La protección de la seguridad nacional para el gobierno de EE. UU depende principalmente de la ciberseguridad, en los documentos y discursos analizados se puede ver reiteradamente la asociación entre aumentar ciberseguridad para protegerse en el ciberespacio como una acción de carácter crítico para la lograr mantener la seguridad nacional. Debido, a que gran parte de la prosperidad económica en este nuevo siglo depende de la ciberseguridad que el país tenga para operar y hacer uso beneficioso en el ciberespacio. Es por eso, que Obama vio la necesidad de nombrar a la Infraestructura digital y a las redes tecnológicas como un activo nacional estratégico, por lo cual, estas se convirtieron en una prioridad de protección y defensa para el gobierno.

A raíz de las filtraciones de información de WikiLeaks en los documentos analizados, se identificó la creciente importancia de la seguridad y protección de información. Este incidente significó un cambio en los procesos para acceder, almacenar y compartir información confidencial, la cual es vital, para preservar la seguridad nacional y mantener operaciones importantes de diferentes tipos en otros lugares del mundo por medio del uso de tecnologías. La organización despertó la

necesidad y la atención de examinar maneras para mejorar e incrementar la protección de la información por medio de la ciberseguridad y así evitar que incidentes de este tipo vuelvan a ocurrir.

Por otra parte, también se observa en como WikiLeaks incidió de cierta manera en la creación de políticas, estrategias, programas y leyes de ciberseguridad al hacer evidente las vulnerabilidades y deficiencias en protección de las infraestructuras críticas de información y comunicación. Estos hechos corroboraron la declaración de Obama en la que se refirió a que los EE. UU no se encontraban lo suficientemente preparados para afrontar los riesgos y amenazas que se producen en el ciberespacio. En aquel entonces, dentro del gobierno estadounidense no existía un funcionario que se encargue de supervisar la política de seguridad cibernética, tampoco, ninguna agencia tenía la responsabilidad o autoridad de analizar el alcance y la escala del desafío cibernético en todo el gobierno. Aunque las acciones de WikiLeaks no fueron las únicas que inspiraron políticas, estrategias, programas y leyes de ciberseguridad a lo largo del mandato de Obama, estas sí contribuyeron a mostrar al gobierno el reto que tenían para crear planes e iniciativas de respuesta frente a incidentes cibernéticos para reducir los efectos y fomentar la recuperación rápida ante los incidentes que se pueden producir en el ciberespacio.

La tercera categoría que corresponde a las acciones anti hegemónicas de actores no estatales transnacionales y los peligros en el ciberespacio sobresalen los siguientes códigos que fueron seleccionados en esta categoría, por su, referencia al entorno y a los elementos que conforman el ciberespacio como: amenazas cibernéticas con 10 repeticiones, hackers con 9 repeticiones, globalización, empoderamiento de actores no estatales en el ciberespacio con 3 repeticiones. Esta categoría obtuvo 41 expresiones que representan el 24% sobre el 100%, lo que quiere decir, que es el segundo porcentaje

más alto que representa la relevancia de como las acciones anti hegemónicas por parte de actores no estatales como WikiLeaks incidieron en la creación de políticas y agencias de ciberseguridad (Ver tabla 4.2: 112).

Esto se evidencia en los documentos recolectados en donde se observa que la palabra amenazas cibernéticas se relaciona a las diferentes acciones que son ocasionadas en el ciberespacio para causar efectos disruptivos, por diferentes actores desde grupos criminales, hackers hasta Estados tecnológicamente avanzados, los cuales, tienen las posibilidades de ejercer acciones disruptivas como robo de información confidencial, ataques cibernéticos para dañar redes, robo de propiedad intelectual, datos financieros entre otras acciones que causan afectaciones principalmente en la seguridad, en el crecimiento económico, y  al bienestar de la sociedad que depende diariamente al ciberespacio. La organización WikiLeaks se asocia a las amenazas cibernéticas por sus características y acciones que ha empleado en el ciberespacio contra EE. UU. En los documentos revisados para esta investigación se ha encontrado que poco después de las filtraciones de información entre el 2010 - 2011 el gobierno estadounidense dijo en reiteradas ocasiones que el país se enfrenta a una amenaza cibernética continua y creciente, por lo cual, asegurar el ciberespacio se convirtió en una de las misiones más importantes para la nación.

La presencia de nuevos actores toma importancia, debido, al rol que llegan a tener dentro del ciberespacio. En donde, se empoderan y logran ataques cibernéticos que son más fáciles que los ataques físicos a un país como EE. UU. Es por eso, que a partir de las acciones con el impacto mediático que obtuvo WikiLeaks con sus filtraciones sirvió a que la administración de Obama como ninguna otra se preocupe de la importancia del ciberespacio para el crecimiento de la nación en diferentes aspectos en la era digital del siglo XXI. En el cual, la globalización ha generado el crecimiento de

las interacciones sociales, económicas, políticas, culturales en todo el mundo, pero también, ha incentivado a que aparezcan nuevas redes de amenazas globales que cada vez avanzan más tecnológicamente, lo que, hace que tengan cada vez más poder destructivo.

Además, la globalización ha formado la nueva realidad internacional. En la cual el transnacionalismo de actores estatales como no estatales han tomado más relevancia en el contexto de las relaciones internacionales. Es por eso, que los documentos analizados hacen referencia especialmente a actores no estatales los cuales el gobierno se refiere a estos actores como hackers en sentido de que son criminales tecnológicos y son los principales enemigos en el ciberespacio. Al estar conscientes de este tipo de actores y sus acciones subversivas el gobierno estadounidense tuvo la necesidad de implementar por primera vez planes y estrategias para combatir en contra del crimen organizado de carácter transnacional. Para EE. UU la organización WikiLeaks es un grupo de cibercriminales e incluso considerados como terroristas de alta tecnología que solo buscaban afectar a la seguridad nacional, a raíz, de las filtraciones WikiLeaks incidió en que EE. UU busque maneras para reforzar las leyes para perseguir y sancionar acciones maliciosas producidas en el ciberespacio.

De acuerdo a lo analizado en este capítulo para llegar a identificar la influencia de la organización transnacional WikiLeaks, que, por medio de sus acciones anti hegemónicas las cuales se basaron en la obtención y publicación de información confidencial del gobierno de EE. UU provocaron la creación de políticas y agencias de ciberseguridad que fortalecieron a la hegemonía estadounidense durante el período 2010- 2015.

Principalmente se identificó que la ciberseguridad durante el período de estudio tomó mucha relevancia, por lo tanto, aumentó a diferencia de años anteriores en los

cuales EE. UU no había sido víctima de robo de información confidencial por medio del uso de herramientas tecnológicas. Sin embargo, se encontró mayor incidencia de WikiLeaks en la creación de políticas, iniciativas y estrategias de ciberseguridad que se enfocaban específicamente solo en la protección de información confidencial y en implementar reformas y planes que incrementen la ciberseguridad de las infraestructuras críticas de información del gobierno para evitar que vuelvan a ocurrir fugas de información.

Se identificó que WikiLeaks despertó aún más la importancia de la ciberseguridad, aunque el impactó que generaron las filtraciones fueron a corto plazo especialmente entre el 2010 – 2011. También, a lo largo del período de investigación se vio el impacto de diferentes acciones anti hegemónicas por otros actores estatales y no estatales en el ciberespacio contra EE. UU, lo que constituyó también como un factor externo en la motivación para crear nuevas políticas, planes y agencias de ciberseguridad. Es por eso, que se debe mencionar que WikiLeaks no fue la única organización que intentó entrar en las infraestructuras críticas de información de la nación ya que, se identificaron otros casos y tipos de ataques cibernéticos a instituciones financieras, otras empresas públicas y privadas, y a distintos ciudadanos, esto ayudó a incrementar la consciencia sobre la importancia y el rol de la ciberseguridad para el país.

Por último, en la categoría del fortalecimiento de la hegemonía fue la que presentó el menor porcentaje de solo el 12%, con esto se pudo identificar en los documentos analizados que EE. UU por medio del incremento de medidas de ciberseguridad tanto como a nivel nacional e internacional fue una manera de impulsar y mantener liderazgo en este dominio ya que, EE. UU es un país que se ha caracterizado por ser un Estado pionero en avance e innovación tecnológica. Desde, las publicaciones

de WikiLeaks las que mostraron las vulnerabilidades en seguridad que afrontaba la nación, esto dio indicios para que el gobierno reflexione sobre la importancia de la seguridad de la información en el ciberespacio. No obstante, se debe resaltar que los sucesos de WikiLeaks no llegaron a ser el factor principal para que EE. UU se concentré en aumentar capacidades cibernéticas que fortalezcan a la nación en términos de poder y seguridad.

No se ha podido comprobar que WikiLeaks haya causado influencia directa o indirecta en la hegemonía, pero, lo que se puede identificar es que de cierta manera esta se fortaleció, debido a que, EE. UU es una nación preponderante en innovación tecnológica para el ciberespacio, además, durante la investigación se puede asociar en como ha hecho uso de estrategias combinadas de poder blando y duro, pero con elementos tecnológicos en el ciberespacio para lograr mantener un cierto orden y preponderancia dentro de este nuevo dominio. En el 2011 impulsó y lideró estrategias por primera vez de alcance internacional con el fin de incrementar la cooperación y la unión en este ámbito, que es, relativamente nuevo para los Estados. La idea de llevar este liderazgo internacionalmente demuestra el poder blando de influencia que necesitaba ejercer para que otros Estados y actores acaten su visión y liderazgo para tener más poder y control sobre el ciberespacio.

Las numerosas filtraciones de WikiLeaks sirvieron para alertar al gobierno sobre los riesgos que existen en el ciberespacio y como el poder por la globalización está en constante cambio y depende del contexto en el que se encuentre, por eso, toma importancia el uso del ciberpoder y el aumento de la ciberseguridad para la nueva dinámica del poder en el siglo XXI. A partir, de la aparición de WikiLeaks la administración de Obama comprendió, aún más, que las capacidades cibernéticas son claves para el dominio de EE. UU.

Entonces, por estos resultados mencionados a lo largo del capítulo se llegó a comprobar que la hipótesis planteada para esta investigación se cumple de forma parcial.

*Tabla 4.1 Libro de códigos*

| Categorías | Características |
|---|---|
| **Fortalecimiento de la hegemonía** | • Un Estado es lo suficientemente poderoso como para mantener las reglas esenciales que rigen las relaciones interestatales y está dispuesto a hacerlo" (Keohane & Nye, 1977)<br>• Uso de poder duro y el poder blando como una alternativa a los propuestos realistas para conservar la hegemonía y ganar poder en el nuevo contexto internacional (Keohane & Nye, 1971).<br>• La potencia hegemónica procura persuadir a los otros de que satisfagan su visión de orden mundial y acaten su liderazgo (Keohane,1984)<br>• El poder depende del contexto y por lo tanto el rápido crecimiento del ciberespacio es un importante nuevo contexto en la política mundial (Nye, 2010) |
| **Aumento de ciberseguridad** | • La constante innovación tecnológica vuelven a las amenazas cada vez más especializadas y difíciles de identificar, lo que motiva y causa que los Estados alcancen nuevas dimensiones en seguridad nacional (Choucri, 2013)<br>• Politización y la disrupción del ciberespacio (Choucri, 2013)<br>• Lograr operaciones en el ciberespacio ofensivas/proactivas y defensivas/ protectivas (Kuehl, 2009).<br>• Desarrollo de estrategias para el ciberespacio es crear recursos y procedimientos cibernéticos que contribuyen al logro de objetivos específicos de seguridad nacional (Kuehl, 2009).<br>• La apertura y popularización de la tecnología tiene innegables implicaciones políticas, debido a que el fácil y barato acceso al internet puede llevar a un posible cambio en la balanza de poder (Nye, 2014)<br>• Cyber superioridad: se refiere al grado en que un actor puede obtener ventaja del uso del ciberespacio y, si es necesario, evitar que el actor adversario obtenga ventaja de él (Kuehl, 2009). |
| **Acciones anti hegemónicas de actores no estatales transnacionales y los peligros en el ciberespacio** | • El surgimiento de un nuevo orden internacional que está regido por la globalización (Nye, 2004)<br>• Hacktivistas, es decir, es un grupo de individuos que hacen uso de los recursos del ciberespacio para generar protestas, promover alguna ideología, e impactar en las agendas políticas de manera legal o quizás más comúnmente ilegal (Sigholm, 2013,)<br>• El surgimiento y empoderamiento de estos nuevos actores hacen que se rompa la lógica tradicional de las relaciones interestatales por la pluralidad y multiplicidad de actores no estatales (Keohane & Nye, 1971).<br>• El poder el cual se vuelve más complejo por los avances tecnológicos, aparición de nuevos actores en el contexto de creciente interdependencia y globalización (Keohane & Nye, 1977).<br>• El internet por sus bajos costos de acceso ha hecho posible las comunicaciones transnacionales entre millones de personas (Nye, 2004)<br>• El ciberespacio ha creado nuevas maneras de comunicación, empoderamiento de individuos y de actores no estatales lo que ha incrementado el rol del poder blando (Nye,2004)<br>• La actividad transnacional hace que las sociedades sean más sensibles unas a otras. Esto puede impulsar a que los gobiernos incrementen sus esfuerzos para controlar este comportamiento no estatal transnacional (Keohane & Nye, 2004)<br>• Los actores transnacionales son definidos como grupos privados que no tienen control por órganos gubernamentales y cuentan con presencia global por lo que desarrollan sus actividades por medio de interacciones y relaciones transnacionales que tienen lugar a través de las fronteras de los Estados, estas se las puede entender como movimientos de información, capital, personas, productos y servicios (Keohane & Nye, 1971) |

Elaborado por: Torres, P. (2020)

*Tabla 4.2 Porcentaje del Análisis de contenido por categoría*

| Categoria | Frecuencia Valorativa (Número de expresiones) | Frecuencia Proporcional (Porcentajes) |
|---|---|---|
| Fortalecimiento de hegemonía | 20 | 12% |
| Aumento de Ciberseguridad | 108 | 64% |
| Acciones antihegemónicas de actores no estatales transnacionales y los peligros en el ciberespacio | 41 | 24% |
| **Total** | 169 | 100% |

Fuente: Torres. P, 2020
Elaborado por: Torres. P, 2020

*Tabla 4.3 Análisis de contenido frecuencia por códigos y categorías*

| Categoría | Códigos | Total de repeticiones | % |
|---|---|---|---|
| **Fortalecimiento de hegemonía** | Prestigio internacional | 4 | 2% |
| | Liderazgo en el ciberespacio | 7 | 4% |
| | Ciberespacio nuevo dominio de poder | 1 | 1% |
| | Ciberpoder | 8 | 5% |
| **Aumento de ciberseguridad** | Ciberseguridad para proteger información de intrusos externos | 3 | 2% |
| | Concientización sobre la importancia de la ciberseguridad poder | 4 | 2% |
| | Cooperación en ciberseguridad | 2 | 1% |
| | Encontrar vulnerabilidades y fallas en las redes del gobierno | 2 | 1% |
| | Especialistas en ciberseguridad para evaluar riesgos y amenazas cibernéticas | 6 | 4% |
| | Fortalecimiento en todo aspecto de la Ciberseguridad | 4 | 2% |

| | | | |
|---|---|---|---|
| | Innovación tecnológica en ciberseguridad | 18 | 11% |
| | Instituciones de Ciberseguridad | 1 | 1% |
| | Inversión en tecnología | 3 | 2% |
| | Mayor preparación en ciberseguridad | 3 | 2% |
| | Nuevo personal del gobierno enfocado en ciberseguridad | 2 | 1% |
| | Políticas, estrategias, programas y leyes de ciberseguridad | 9 | 5% |
| | Prevención y detención de ataques cibernéticos | 4 | 2% |
| | Protección de la nación en el ciberespacio | 5 | 3% |
| | Proteger la seguridad nacional | 9 | 5% |
| | Reformas y revisiones en políticas sobre protección y seguridad de infraestructuras críticas de información | 14 | 8% |
| | Reformas, revisiones y pruebas sobre los procesos de manejo de información confidencial en las redes del gobierno | 1 | 1% |
| | Respuestas a incidentes cibernéticos | 4 | 2% |
| | Revisión de las prácticas de seguridad | 4 | 2% |
| | Seguridad y protección de información | 10 | 6% |
| **Acciones antihegemónicas de actores no estatales transnacionales y los peligros en el ciberespacio** | Afectaciones a la Seguridad Nacional | 3 | 2% |
| | Afectaciones a las estrategias de EE. UU | 2 | 1% |
| | Amenazas cibernéticas | 10 | 6% |
| | Ataques cibernéticos y acciones disruptivas | 2 | 1% |
| | Efectos disruptivos | 2 | 1% |
| | Empoderamiento de actores no estatales en el ciberespacio | 3 | 2% |

| | | | |
|---|---|---|---|
| | Filtración de información confidencial | 3 | 2% |
| | Globalización | 6 | 4% |
| | Hackers | 9 | 5% |
| | Riesgos de la filtración de información | 1 | 1% |
| **TOTAL** | | 169 | 100% |

Fuente: Torres. P, 2020
Elaborado por: Torres. P, 2020

## VII. CONCLUSIONES

En base a la hipótesis y a los objetivos propuestos en el presente trabajo de disertación se han formulado las siguientes conclusiones:

- La hipótesis planteada para esta investigación: "la organización transnacional WikiLeaks, por medio de sus acciones anti-hegemónicas en el ciberespacio, provocó la creación de políticas y agencias de ciberseguridad que fortalecieron a la hegemonía estadounidense en el período 2010-2015" se cumple parcialmente debido a que se identificó que WikiLeaks no fue el factor principal que provocó que EE. UU incremente nuevas políticas y agencias de ciberseguridad durante el período de esta investigación, tampoco la organización causó directamente el fortalecimiento de la hegemonía de este país. No obstante, se debe recalcar que la hegemonía de EE. UU se ha fortalecido gracias a la importancia que le ha dado esta nación a aumentar capacidades cibernéticas para operar con más poder dentro del ciberespacio, lo que le ha permitido expandir y fortalecer su soberanía dentro de este dominio, debido a que ha tomado el liderazgo para promover iniciativas de alcance internacional con el fin de establecer planes, directrices y acuerdos comunes con otras naciones y organismos sobre el uso del ciberespacio.
- Las revelaciones de WikiLeaks tuvieron solo un efecto de gran impacto mediático a corto plazo, aunque no hay evidencia en que hayan llegado a causar daños a la seguridad nacional y en las relaciones internacionales del país. Estos sucesos si marcaron un precedente en que EE. UU se haya concientizado aún más sobre la importancia de las actuaciones de los nuevos actores que emergen en el ciberespacio, y, por lo tanto, se preocupó en establecer un grupo de trabajo sobre WikiLeaks el cual tenía que abordar los problemas de las políticas sobre la

garantía de la información, asuntos legales, seguridad, contrainteligencia por la revelación de estos documentos.

- A raíz de las filtraciones se nombró a Russell Travers como Asesor Principal del Personal de Seguridad Nacional para el acceso a información y política de Seguridad al cual se le encargo la tarea de liderar un esfuerzo integral para identificar y desarrollar las reformas estructurales que sean necesarias por las filtraciones de información confidencial por WikiLeaks. Este incidente destacó la importancia de incrementar mayor vigilancia, es por eso, que las agencias que operaban redes o sistemas de información clasificada fueron sometidas a una exhaustiva evaluación de seguridad con expertos en contrainteligencia y de aseguramiento de información con el fin de implementar cambios que aseguren altos niveles de protección para la información clasificada.
- WikiLeaks también impulsó a que el gobierno esté consciente de que la prevención para evitar divulgaciones no autorizadas de información confidencial y clasificada del gobierno debe ser una prioridad en cada agencia federal. Es por esto, que el presidente Obama emitió la Orden Ejecutiva 13587 sobre reformas estructurales para mejorar la seguridad de las redes clasificadas, el intercambio responsable y la salvaguarda de la información clasificada. Además, por medio de esta orden se estableció un grupo de trabajo sobre amenazas internas el que desarrolló un programa para disuadir, detectar y mitigar las amenazas internas en todo el gobierno.
- Las filtraciones del 2010 causaron la politización de la ciberseguridad en todo el gobierno y establecieron la agenda estatal de EE. UU durante ese año que se enfocó en la importancia de las amenazas cibernéticas y como combatirlas, debido a que, la seguridad nacional del país pasó a depender de la

implementación de medidas de ciberseguridad y aumentó de capacidades cibernéticas.

- En el 2010 se evidenció aún más la importancia del ciberespacio, esto se pudo notar en la Estrategia de Seguridad Nacional (2010), la cual fue la primera estrategia de este país que le dio énfasis a las "amenazas cibernéticas" y el terminó de "espacio cibernético" o ciberespacio apareció por primera vez con la connotación de ser una de las más graves amenazas a la seguridad nacional.
- La administración de Barack Obama se destacó por la gran importancia que le dio a la protección de la infraestructura digital de EE. UU y al incremento de tecnologías de información y comunicación que sean más fuertes y resistentes, por esto para reafirmar su compromiso con la seguridad de la nación el Presidente nombró a las redes de EE. UU como activos nacionales estratégicos, y su defensa se convirtió en una prioridad de seguridad nacional.
- Se evidenció el poder de influencia o blando de EE. UU en su misma población, debido a que el gobierno promovió su discurso en contra de WikiLeaks y amenazas cibernéticas, esto se vio reflejado en los resultados de las encuestas a ciudadanos estadounidenses realizadas poco después de las filtraciones los resultados indicaron que la mayoría tenía la percepción de que WikiLeaks pone en riesgo la seguridad nacional y perjudica las relaciones internacionales de los Estados Unidos.
- Estados Unidos es un país con una gran capacidad de ejercer *soft power*, además, por medio de este logra conservar la hegemonía. Es por esto, que su liderazgo se ha visto reflejado en otros organismos internacionales los cuales han impulsado propuestas en ciberseguridad con enfoques muy similares a los que EE. UU ha creado en sus estrategias de alcance internacional.

- Estados Unidos ha fortalecido su hegemonía al ser un país que ha generado y liderado numerosas iniciativas frente a los problemas y peligros del ciberespacio en los últimos once años. Al darse cuenta, no solo por los sucesos con WikiLeaks que es vulnerable en este dominio ha visto la importancia de incrementar e innovar constantemente en capacidades cibernéticas las cuales son clave para tener dominio dentro del ciberespacio, con estas estrategias la nación también ha obtenido legitimidad por parte de la comunidad internacional lo que le ayuda a adquirir más poder.
- La globalización ha tenido un papel fundamental al desarrollar herramientas claves para el progreso de las sociedades como el ciberespacio que a lo largo de los últimos años ha creado una gran dependencia para todos desde individuos hasta los Estados, es por esto, que la difusión y expansión del internet ha brindado la oportunidad de que surjan amenazas de todo tipo dentro de este dominio, el cual es un entorno en donde desde las fuerzas militares y la sociedad en general que abarca lo (político, negocios, educación y diferentes tipos interacciones transnacionales) han empezado a aprender como operar dentro de este espacio.
- La globalización, también ha sido un factor importante para los cambios en la balanza del poder gracias a la apertura y popularización de la Tecnología, lo que, ha causado baratos costos y pocas barreras de entrada a diferentes tipos de actores, el ciberespacio se ha convertido en un lugar de empoderamiento. Esto refleja la difusión del poder que se refiere al movimiento de este entre los Estados a actores no estatales, lo que brinda la posibilidad a todos los actores a usar recursos de poder blando y duro dentro del contexto tecnológico y cibernético, lo que resulta en un poder cibernético. Por eso,

WikiLeaks es un actor que mostró su empoderamiento en el ciberespacio por medio de sus capacidades para recibir y distribuir información filtrada de manera barata, rápida con el fin de lograr el mayor impacto político e influir a las sociedades con su objetivo de llevar la transparencia de información.

## VIII. RECOMENDACIONES

- El constante desarrollo e innovación tecnológica han significado innegables cambios en el poder, el internet ha formado un nuevo contexto en la realidad de los individuos con repercusión en las relaciones internacionales. Es por eso, que se recomienda ampliar más lo conocimientos e ideas que han surgido de este trabajo de investigación, debido a que la temática sobre el desarrollo del ciberespacio es reciente y se encuentra en constante evolución, por eso, es importante seguir actualizando información sobre las dificultades, amenazas y oportunidades que presenta este dominio para los Estados. Para actualizar información y conocimientos sobre el espacio cibernético se recomienda que los Estados apoyen y fomenten la educación en este ámbito tecnológico, el cual se puede llevar a cabo por medio de cooperación con otros gobiernos u organismos especializados en temas sobre el ciberespacio con los cuales puedan llegar a acuerdos para que ofrezcan becas en carreras con enfoque en las tecnologías de información y comunicación y ciberseguridad.
- El ciberespacio es un dominio complejo en el cual los Estados tienen que buscar estrategias para operar con seguridad y lograr diferentes objetivos dentro de él. Para esto es fundamental que los Estados se enfoquen en otorgar mayor inversión a recursos de educación tecnológica para el ciberespacio, de esta manera van a poder formar personal capacitado para analizar y operar frente a

las oportunidades y riesgos que se presentan en este nuevo dominio en el presente y en el futuro.

- Se debe resaltar que el internet ha permitido a los Estados obtener más información, comunicación y mayor interacción lo que resulta en Estados con más poder, pero que a la vez son vulnerables dentro del ciberespacio, debido a que otros actores toman un rol importante ya que, sus acciones pueden llegar a lograr ataques efectivos a bajo costo, por esto es recomendable implementar campañas de concientización en medios de comunicación y en redes sociales sobre los usos del ciberespacio para tratar de evitar que individuos provoquen incidentes cibernéticos que afecten a la nación y a sus habitantes.
- El ciberespacio y la ciberseguridad representan desafíos complejos y para lograrlos se necesita impulsar voluntad política por parte de diferentes Estados, aún hace falta implementar una estrategia global de ciberseguridad con enfoque en el desarrollo de infraestructuras de información que lideren el ciberespacio, la cual debe ser coherente, sólida y efectiva ya que, tiene que responder a las necesidades de seguridad de las infraestructuras de información para que de esta manera incrementar confianza e impulsar bienestar social y económico que beneficie a todos.
- Para explorar a más profundidad y precisión las motivaciones del gobierno estadounidense para incrementar iniciativas ciberseguridad se recomiendan usar el método análisis crítico del discurso debido a que es una técnica más compleja de la investigación cualitativa, que permite ver a más detalle las micro estructuras que forman parte de los discursos, esto ayuda al investigador a adoptar una posición con el objetivo de descubrir, interpretar, desmitificar y, al

mismo tiempo, poder desafiar y comprender mejor una posición en temas relacionados con el poder.

- Por último, se recomienda que para futuras investigaciones similares con metodología cualitativa se realice previamente un procedimiento de selección de la información el cual permita identificar la relevancia y observar los detalles específicos acorde al tema, es importante recalcar esto ya que, el método empleado presentó limitaciones debido a la cuantiosa y sesgada información que se puede encontrar. Se recomienda usar recursos más tecnológicos, por ejemplo, un software de computadora para análisis de datos cualitativos los cuales permiten analizar mayor cantidad de textos y el proceso de codificación se vuelve más especializado.

## LISTA DE REFERENCIAS

**Tesis:**


Armstrong, E. (2015). The Politics of Information: Examining the Conflict Between WikiLeaks and the US Government. Recuperado de: https://pdfs.semanticscholar.org/1d2e/fda7b021c7058750b7f56ced0dedcf15dd71.pdf

Charme, A. (2014). Efecto de WikiLeaks en Relaciones Internacionales: el caso del Departamento de Estado estadounidense y alemán. Recuperado de http://www.academia.edu/8894979/Efecto_de_WikiLeaks_en_Relaciones_Internacionales_el_caso_del_Departamento_de_Estado_estadounidense_y_alem%C3%A1n

Conde, A. (2014). Cablegate: Las consecuencias diplomáticas de WikiLeaks en la relación bilateral México- Estados Unido. El colegio de México. Recuperado el 24 de Diciembre de 2019, de Centro de Estudios Internacionales: https://books.google.com.ec/books/about/Cablegate.html?id=qSF6oAEACAAJ&redir_esc=y

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

Nardoianni, M. (2016). The Cyber Security Challenge: A Comparative Analysis. Recuperado de: https://tesi.luiss.it/19114/1/624562_NARDOIANNI_MARIA%20GRAZIA.pdf

Navarro, T., (2009). Un cambio de la naturaleza hegemónica del mundo. Universidad de las Américas Puebla. Recuperado de http://catarina.udlap.mx/u_dl_a/tales/documentos/lri/navarro_m_tk/capitulo_1.html

Quian, A. (2016). Impacto mediático y político del activismo hacker en la sociedad red. Estudio de caso: Wikileaks. diciembre 20, 2019, de Universidad Carlos III de Madrid. Departamento de Periodismo y Comunicación Audiovisual Sitio web: http://hdl.handle.net/10016/23221

Rodríguez, E., & Cordero, A. (2018). Ciberseguridad : los acuerdos de cooperación para el tratamiento de las amenazas en el ciberespacio. El caso de Estados Unidos y China. Universidad de la Salle Ciencia Unisalle. Recuperado el 20 de Enero de 2020, de https://ciencia.lasalle.edu.co/cgi/viewcontent.cgi?article=1083&context=negocios_relaciones

Torres, F., (2018). El poder blando como herramienta generadora de influencia en un mundo globalizado. El colegio de San Luis A.C. Recuperado de https://biblio.colsan.edu.mx/tesis/LRI_TorresCastilloFranciscoGuadalupe.pdf

Villalba, A. (2015). La ciberseguridad en España 2011–2015 una propuesta de modelo de organización . Universidad Nacional de Educación a Distancia. España. Recuperado de: http://e-spacio.uned.es/fez/eserv/tesisuned:CiencPolSoc-Avillalba/VILLALBA_FERNANDEZ_Anibal_Tesis.pdf

**Sitios Web:**

Bowman, B. ( 2019). Which Country is #1 in Cybersecurity?Security Boulevard. Recuperado el 28 de Enero de 2020, de https://securityboulevard.com/2019/07/which-country-is-1-in-cybersecurity/

BSCF. (2011). Blueprint for a secure cyberfuture. Department of Homeland Security. Recuperado el 22 de Enero de 2020, de https://www.dhs.gov/xlibrary/assets/nppd/blueprint-for-a-secure-cyber-future.pdf

Chrisafis, A. (2011). Zine al-Abidine Ben Ali forced to flee Tunisia as protesters claim victory. Recuperado The Guardian el 26 de Diciembre de 2019, de https://www.theguardian.com/world/2011/jan/14/tunisian-president-flees-country-protests

CISA. (2009). Cyber Storm: Securing Cyber Space. Recuperado de Cybersecurity and Infrastructure Security Agency. https://www.cisa.gov/cyber-storm-iii

CISA. (2018). Cybersecurity and Infrastructure Security Agency (CISA). Recuperado el 31 de Enero de 2020, de https://www.us-cert.gov/about-us

CNCI. (2011). Department of Homeland Security. Obtenido de NCIRP: https://federalnewsnetwork.com/wp-content/uploads/pdfs/NCIRP_Interim_Version_September_2010.pdf

Confidencial, E. (2010). El Confidencial. Recuperado el 23 de Diciembre de 2019, de https://www.elconfidencial.com/mundo/2010-07-27/las-filtraciones-revolucionan-a-los-gobiernos-presentes-en-afganistan_299985/

CTIIC. (2015). Office of the Director of National Intelligence. Recuperado el 31 de Enero de 2020, de Cyber Threat Intelligence Integration Center: https://www.dni.gov/index.php/ctiic-who-we-are

DHS. (2011). Combating Transnational Organized Crime. Department of Homeland Security. Recuperado el 24 de Enero de 2020, de https://www.dhs.gov/blog/2011/07/25/combating-transnational-organized-crime

Garamone,. J. (2010). Officials condemn leaks, detail prevention efforts. American Forces Press Service Recuperado de https://www.army.mil/article/48688/officials_condemn_leaks_detail_prevention_efforts

Gibney., A., Schmuger, M., Bloom, A. (productores) y Gibney., A. (director). (2013). We Steal Secrets: The Story of WikiLeaks {documental}. United States. Jigsaw Productions Global Produce

Gosztola, K. (2011). Shadow Proof. Recuperado el 26 de Diciembre de 2019, de https://shadowproof.com/2011/07/25/reflecting-on-the-afghanistan-war-logs-released-by-wikileaks-one-year-ago/

HSDL. (2011). Homeland Security Digital Library. Recuperado el 24 de Enero de 2020, de https://obamawhitehouse.archives.gov/sites/default/files/Strategy_to_Combat_Transnational_Organized_Crime_July_2011.pdf

ITU. (2007). International Tecnology Union. Recuperado el 23 de Enero de 2020, de https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx

ITU. (2011). International Telecommunication Union. Recuperado el 23 de Enero de 2020, de https://www.unodc.org/documents/treaties/organized_crime/EGM_cybercrime_2011/Presentations/ITU_Cybercrime_EGMJan2011.pdf

Landler, M. (2011). U.S. Sends Warning to People Named in Cable Leaks Recuperado de The New York Times, el 26 de Diciembre de 2019: https://www.nytimes.com/2011/01/07/world/07wiki.html?pagewanted=print

Narváez, F. (2012). Agencia Latinoamericana de Información. Recuperado el 23 de Diciembre de 2019, de https://www.alainet.org/es/active/51829#_ftn17

National Insider Threat Task Force NITTF (2011). Establishment of NITTF. Recupearado de The National Counterintelligence and Security Center. https://www.dni.gov/index.php/ncsc-how-we-work/ncsc-nittf

NCIRP. (2010). Department of Homeland Security. Recuperado el 22 de Enero de 2020, de https://federalnewsnetwork.com/wp-content/uploads/pdfs/NCIRP_Interim_Version_September_2010.pdf

NSA. (2018). National Security Agency, NSA - What We Do. Recuperado el 31 de Enero de 2020, de https://www.nsa.gov/what-we-do

NSS. (2010). Obama White House Archives. Recuperado el 24 de Enero de 2020, de https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/national_security_strategy.pdf

OECD. (2010). Organisation for economic co-operation and Development. Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy and Non-governmental Perspectives on a New Generation of National Cybersecurity Strategies: Contributions from BIAC, CSISAC and ITAC. Recuperado de https://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf

ONU. (2013). Organización de las Naciones Unidas. Obtenido de https://www.un.org/disarmament/ict-security/

Packer, G. (2010). The New Yorker. Recuperado el 26 de Diciembre de 2019, de https://www.newyorker.com/news/george-packer/the-right-to-secrecy

Pellerin, C. (2011). DoD releases first strategy for operating in cyberspace. U.S. Army. Recuperado el 21 de Enero de 2020, de https://www.army.mil/article/61720/dod_releases_first_strategy_for_operating_in_cyberspace

QHSR. (2010). Quadrennial Homeland Security Review. Recuperado de Department of Homeland Security el 22 de Enero de 2020, de https://www.dhs.gov/xlibrary/assets/qhsr_report.pdf

SOC. (2011). Department of Defense. Recuperado el 2020 de Enero de 2020, de https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf

Wikileaks, (2015). What is Wikileaks. Recuperado de https://wikileaks.org/What-is-WikiLeaks.html

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

The New York Times (2009). Obama's Speech on N.S.A. Phone Surveillance. Recuperado de https://www.nytimes.com/2014/01/18/us/politics/obamas-speech-on-nsa-phone-surveillance.html

C-SPAN, (2010). Presidential Remarks on WikiLeaks Release of Classified Documents. Recuperado de https://www.c-span.org/video/?294779-1/presidential-remarks-wikileaks-release-classified-documents

**Revistas Electrónicas:**

Albarez. N., (2016). El concepto de Hegemonía en Gramsci: Una propuesta para el análisis y la acción política. Revista Estudios Sociales Contemporáneos. Recuperado de https://bdigital.uncu.edu.ar/objetos_digitales/9093/08-albarez-esc15-2017.pdf

Díaz, C., (2018). Investigación cualitativa y análisis de contenido temático. Orientación intelectual de revista Universum. Revista General de Información y Documentación https://revistas.ucm.es/index.php/RGID/article/download/60813/4564456547606/0

Gomes de Assis, C. (2017). La nueva era de la información como poder y el campo de la ciberinteligencia. Recuperado de Revista de Estudios de Seguridad URVIO https://revistas.flacsoandes.edu.ec/urvio/article/view/2577

González, J.L. (2010). Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio. Ministerio de Defensa cuaderno de estrategia 149. Instituto Español de Estudios Estratégicos. Recuperado de http://www.ieee.es/Galerias/fichero/cuadernos/CE_149_Ciberseguridad.pdf

Herrera, D.(2017). Hegemonía y relaciones internacionales un estado del arte. Recuperado de Revista de Relaciones Internacionales de la UNAM: http://www.revistas.unam.mx/index.php/rri/article/view/61145

La Porte, T. (2016). Influencia de los actores internacionales no-estatales en las estrategias diplomáticas: consideraciones desde la comunicación pública. Comillas Journal of International Relations, Recuperado de https://revistas.comillas.edu/index.php/internationalrelations/article/view/6960/6774

Morales, D. (2012). Poder suave en relaciones internacionales: Entre propagandistas, estrategas, críticos y escépticos. Revista Contextualizaciones Latinoamericanas. Recuperado de http://www.revistascientificas.udg.mx/index.php/CL/article/download/2812/2554

Quian, A., Carlos, E., (2018). Estrategias y razones del impacto de WikiLeaks en la opinión pública mundial. Recuperado de Revista Española de Investigaciones Sociológicas, 162: 91-110. https://dialnet.unirioja.es/servlet/articulo?codigo=6388204

Sánchez, C. (2011). Analogías de la historia: Julian assange y Wikileaks vs Daniel Ellsberg y los pentagon papers. Nómadas: Critical Journal of Social and Juridical Sciences, 27-48. Recuperado el 24 de Diciembre de 2019, de https://dialnet.unirioja.es/servlet/articulo?codigo=4143175

Schackelford, S., & Craig, A. (7 de Junio de 2014). Beyond the New 'Digital Divide': Analyzing the Evolving Role of National Governments in Internet Governance and Enhancing Cybersecurity. Stanford Journal of International Law. Obtenido de https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2446666

Sigholm, J., (2013). Non-State Actors in Cyberspace Operations. Journal of Military Studies. Recuperado de https://www.diva-portal.org/smash/get/diva2:611814/FULLTEXT01.pdf

**Artículos electrónicos:**

Abela J.A (2002). Las técnicas de análisis de contenido: una revisión actualizada. Recuperado de: http://www.albertomayol.cl/wp-content/uploads/2014/08/Andreu-Analisis-de-contenido.pdf

Azócar, D., & Lavín, J. (2015). El ciberespacio y las relaciones internacionales en la era digital., Recuperado de: https://www.academia.edu/12269221/El_ciberespacio_y_las_relaciones_internacionales_en_la_era_digital_pre-publicaci%C3%B3n_libro_C%C3%A1tedra_Michel_Foucault_Escuela_Chile-Francia_

Bejarano, M. J. (8 de Junio de 2011). La Estrategia Internacional para el Ciberespacio. Instituto Español de Estudios Estratégicos. Recuperado el 13 de Enero de 2020, de http://www.ieee.es/Galerias/fichero/docs_informativos/2011/DIEEEI21-2011EstrategiaInternacionalCiberespacio.pdf

CCDCOE. (2016). NATO Cooperative Cyber Defence Centre of Excellence. Recuperado el 26 de Diciembre de 2019, de https://ccdcoe.org/uploads/2018/10/CS_organisation_USA_122015.pdf

DeVine, M. (2019). Intelligence Community Spending: Trends and Issues. Congressional Research Service. Recuperado de: https://fas.org/sgp/crs/intel/R44381.pdf

Fenster, M., (2012). *Disclosure's Effects: WikiLeaks and Transparency* , 97 Iowa L. Rev. 753 (2012), *Recuperado de* http://scholarship.law.ufl.edu/facultypub/250

Foreign Policy. (2011). Revolution in the Arab World, 1-227. Recuperado el 26 de Diciembre de 2019, de https://www.scribd.com/doc/51118252/revolution-in-the-arab-world

Kuehl, D. (2002). Information operations, information warfare and computer network attack their relationship to national security in the information age. Recuperado de International Law Studies volume 76. https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=1400&context=ils

Kuehl, D. (2009). Cyberspace & Cyberpower: Defining the Problem. Cyberpower & National Security. Recuperado de https://ndupress.ndu.edu/Portals/68/Documents/Books/CTBSP-Exports/Cyberpower/Cyberpower-I-Chap-02.pdf?ver=2017-06-16-115052-210

Leigh, D., Harding, L.(2011). Inside Julian Assange´s War on Secrecy. Recuperado de http://capitolreader.com/sum/10311-wiki.pdf

Lewis, J., (2016). Experiencias avanzadas en políticas y prácticas de ciberseguridad. Banco Interamericano de Desarrollo. Recuperado de BID https://publications.iadb.org/es/publicacion/17142/experiencias-avanzadas-en-politicas-y-practicas-de-ciberseguridad-panorama

López, F. (2009). El análisis de contenido como método de investigación. Universidad de Huelva. *Revista de Educación*. Recuperado de http://rabida.uhu.es/dspace/bitstream/handle/10272/1912/b15150434.pdf?sequence=1

Masullo, J. (2011). Sobre el poder blando y el biopoder.: Evaluando el potencial impacto y limitaciones de M. Foucault en las RI (pp. 7-14, Rep.). Institut Barcelona d'Estudis Internacionals (IBEI). Retrieved March 23, 2020, from www.jstor.org/stable/resrep14223.5

Muñoz, B. (2013). Seguridad Nacional, definiciones y conceptos. Bibliotecas UDLAP. Recuperado de http://catarina.udlap.mx/u_dl_a/tales/documentos/lri/munoz_p_ba/capitulo_1.html#

Neuendorf, K. (2010). Content Analysis. A methodological primer for gender research. Springer Science. Recuperado de http://academic.csuohio.edu/kneuendorf/c63311/Neuendorf11.pdf

Nye, J. (2010). “Cyber Power.” Paper, Belfer Center for Science and International Affairs, Harvard Kennedy School, Recuperado de https://www.belfercenter.org/publication/cyber-power

Pastor, Ó., Pérez, J. A., Arnáiz de la Torre, D., & Toboso, P. (2009). Seguridad nacional y ciberdefensa. Cátedra Isdefe-UPM. Obtenido de Escuela Técnica Superior de Ingenieros de Telecomunicaciones ETSIT: http://catedraisdefe.etsit.upm.es/wp-content/uploads/2010/07/CUADERNO-N%C2%BA-6.pdf

Porta, L., Silva, M. (2003). La investigación cualitativa: El análisis de contenido en la investigación educativa. Recuperado de http://abacoenred.com/wp-content/uploads/2016/01/An%C3%A1lisis-de-contenido-en-investigaci%C3%B3n-educativa-UNMP-UNPA-2003.pdf.pdf

Saldaña, J. (2013). The coding manual for qualitative researchers. Sage 2013. Recuperado de https://www.sagepub.com/sites/default/files/upm-binaries/24614_01_Saldana_Ch_01.pdf

Starr, S., (2009). Toward a Preliminary Theory of Cyberpower. Recuperado de National Defense University Press- Cyberpower and National Security. https://ndupress.ndu.edu/Media/News/Article/1216674/cyberpower-and-national-security/

Swab, A. (2019). Black Budgets: The U.S. Government’s Secret Military and Intelligence Expenditures. Harvard Law School, Recuperado de: https://scholar.harvard.edu/files/briefingpapers/files/72_-_swab_-_black_budgets.pdf

Vergara, E., Trama, G. (2017) Operaciones militares cibernéticas: planeamiento y ejecución en el nivel operacional. Escuela Superior de Guerra Conjunta de las Fuerzas Armadas. Recuperado de http://www.cefadigital.edu.ar/handle/123456789/939

Vidal, J., Romero, J., (2011). La responsabilidad ética en internet: Wikileaks y la difusión de documentos secretos. Recuperado de Depósito de investigación Universidad de Sevilla https://idus.us.es/xmlui/handle/11441/35101

Yukaruç, U.(2017). A Critical Approach to Soft Power. Bitlis Eren Üniversitesi Sosyal Bilimler Enstitüsü Dergisi / Journal of Bitlis Eren University. Recuperado de https://dergipark.org.tr/tr/download/article-file/393488

Zifcak, S., (2019). The emergence of WikiLeaks: Openness, Secrecy and Democracy. More or Less Democracy and New Media. Recuperado de http://people.exeter.ac.uk/mm394/Spencer_Zifcak.pdf

**Documentos Oficiales:**

Clinton, H. (2010). U.S Department of State. Recuperado el 25 de Diciembre de 2019, de https://2009-2017.state.gov/secretary/20092013clinton/rm/2010/11/152078.htm

CNCI. (2010). Executive Office of the President of the United States. Obtenido de https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-034.pdf

DHS, (2011). Blueprint for a Secure Cyber Future. Recuperado de Department of Homeland Security: https://www.dhs.gov/xlibrary/assets/nppd/blueprint-for-a-secure-cyber-future.pdf

Executive Order 13587. (2011). Obama White House Archives. Recuperado el 14 de Enero de 2020, de https://obamawhitehouse.archives.gov/the-press-office/2011/10/07/executive-order-13587-structural-reforms-improve-security-classified-net

Federal Information Security Management Act FISMA (2011). Fiscal Year 2010 Report to Congress on the Implementation of The Federal Information Security Management Act of 2002. Recuperado de White House https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/assets/egov_docs/FY10_FISMA.pdf

Federal Information Security Management Act FISMA (2012). Fiscal Year 2011 Report to Congress on the Implementation of The Federal Information Security Management Act of 2002. Recuperado de White House https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/assets/egov_docs/fy11_fisma.pdf

Gates, R., Mullen, M., (2010). DOD News Briefing with Secretary Gates and Adm. Mullen from the Pentagon. Recuperado de Department of Defense: https://fas.org/sgp/news/2010/07/dod072910.html

International Strategy for Cyberspace, (2011). Prosperity, Security, and Openness in a Networked World. Seal of the President of the United States. Recuperado de https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

Jones, J. (2010). Statement of National Security Advisor GEN James Jones on Wikileaks. Recuperado de https://www.centcom.mil/MEDIA/NEWS-ARTICLES/News-Article-View/Article/884110/statement-of-national-security-advisor-gen-james-jones-on-wikileaks/

Jones, J. (2010). The President's 2010 National Security Strategy. Recuperado de National Security Advisor https://2009-2017-fpc.state.gov/142282.htm

Kennedy, P. (2011). Homeland Security and Governmental Affairs. Recuperado el 25 de Diciembre de 2019, de https://fas.org/irp/congress/2011_hr/031011kennedy.pdf

Ministerio Español de Defensa. (2010). La estrategia de seguridad nacional de los eeuu “aspectos más destacados de su evolución” instituto español de estudios estratégicos. Recuperado el 22 de Enero de 2020, de http://www.ieee.es/Galerias/fichero/2010/DA-IEEE_06-2010_NSS_2010_ASPECTOS_DESTACADOS_DE_SU_EVOLUCION.pdf

Obama, B., (2011). Strategy to Combat Transnational Organized Crime: Letter from the President. Recuperado de National Security Council.

https://obamawhitehouse.archives.gov/administration/eop/nsc/transnational-crime/letter

Phillips, M., (2009). Introducing the New Cybersecurity Coordinator. Recuperado de The White House https://obamawhitehouse.archives.gov/blog/2009/12/22/introducing-new-cybersecurity-coordinator

PPD-8. (2011). Department of Homeland Security. Recuperado el 14 de Enero de 2020, de https://www.dhs.gov/presidential-policy-directive-8-national-preparedness

Schmidt, H. (2011). Launching the U.S. International Strategy for Cyberspace. The White House. Recuperado el 14 de Enero de 2020, de https://obamawhitehouse.archives.gov/blog/2011/05/16/launching-us-international-strategy-cyberspace

Schmidt, H., (2010). Launching the U.S. International Strategy for Cyberspace. Recuperado de The White House https://obamawhitehouse.archives.gov/blog/2011/05/16/launching-us-international-strategy-cyberspace

Schmidt, H., (2010). Open for Questions: Howard Schmidt on Cyber Security Awareness. Recuperado de The White House https://obamawhitehouse.archives.gov/blog/2010/10/15/open-questions-howard-schmidt-cyber-security-awareness

The White House (2009). President Obama explains how the growth of digital networks has increased the need to invest in online security. Recuperado de https://www.youtube.com/watch?v=UIIY9AQSqbY

The White House (2014). President Obama Discusses U.S. Intelligence Programs at the Department of Justice. Recuperado de https://obamawhitehouse.archives.gov/blog/2014/01/17/president-obama-discusses-us-intelligence-programs-department-justice

The White House (2014). Remarks by the President at the National Cybersecurity Communications Integration Center. Recuperado de https://obamawhitehouse.archives.gov/the-press-office/2015/01/13/remarks-president-national-cybersecurity-communications-integration-cent

The White House (2014). Statement by the President on the Cybersecurity Framework. Recuperado de https://obamawhitehouse.archives.gov/the-press-office/2014/02/12/statement-president-cybersecurity-framework

The White House (2015). Remarks as Prepared for Delivery by Assistant to the President for Homeland Security and Counterterrorism Lisa O. Monaco Strengthening our Nation's Cyber Defenses. Recuperado de https://obamawhitehouse.archives.gov/realitycheck/the-press-office/2015/02/11/remarks-prepared-delivery-assistant-president-homeland-security-and-coun

The White House. (2010). FACT SHEET: U.S. Government Mitigation Efforts in Light of the Recent Unlawful Disclosure of Classified Information. The White House. Recuperado el 25 de Diciembre de 2019, de Office of the Press Secretary:

https://obamawhitehouse.archives.gov/the-press-office/2010/12/01/fact-sheet-us-government-mitigation-efforts-light-recent-unlawful-disclo

Whitman, B., (2010) Remarks on hundreds of thousands of stolen classified State Department documents provided to them by Wilileaks. Recuperado de U.S. Department of Defense Office of the Assistant Secretary of Defense (Public Affairs). https://fas.org/sgp/news/2010/11/dod-wikileaks.html

**Libros Electrónicos:**

Babbie, E.,( 1975). The Practice of Social Research, Thirteenth Edition, International Edition. Recuperado de Chapman University. http://jsp.ruixing.cc/jpkc_xingfa/JC_Data/JC_Edt/lnk/20161105194206236.pdf

Choucri, N. (2013). Cyberpolitics in International Relations. The MIT Press. London, England. Recuperado de: https://flavioufabc.files.wordpress.com/2017/02/cyberpolitics-and-international-relations.pdf

Gramsci, A. (1971). Selections from the Prison Notebooks. Lawrence and Wishart. Recuperado de https://www.lwbooks.co.uk/book/selections-prison-notebooks

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

Keohane R., & Nye, J. (1998). Power and interdependency in the Information Age. Recuperado de http://www.rochelleterman.com/ir/sites/default/files/Keohane%20Nye%202000.pdf

Keohane R., & Nye, J. (2004). Transgovernmental relations and international organizations. Recuperado de Power in a Global Information Age from Realism to Globalization https://edisciplinas.usp.br/pluginfile.php/851660/mod_folder/content/0/NYE.%20Power%20in%20the%20Global%20Information%20Age-%20From%20Realism%20to%20Globalization%20%282004%29.pdf?forcedownload=1

Keohane, R., & Nye, J. (1971). Transnational Relations and World Politics: An Introduction. International Organization. Recuperado de https://sites.google.com/site/wikioeinebrija/distincion-transnacional-interestatal

Keohane., R. (1984). After Hegemony Cooperation and Discord in the World Political Economy. Princenton University Press. Recuperado de https://www.researchgate.net/publication/243721473_After_Hegemony_Cooperation_and_Discord_in_World_Political_Economy

Lukes, S. (1974). Power: A Radical View. Palgrave MacMillan Press. Recuperado de https://voidnetwork.gr/wp-content/uploads/2016/09/Power-A-Radical-View-Steven-Lukes.pdf

Nye, J. (1990). The Changing Nature of World Power. Political Science Quarterly, 105(2), 177-192. Recuperado de https://www.jstor.org/stable/2151022?seq=1

Nye, J. (2004). Power in a Global Information Age from realism to globalization. Recuperado de Taylor & Francis e-Library https://edisciplinas.usp.br/pluginfile.php/851660/mod_folder/content/0/NYE.%20Power%20in%20the%20Global%20Information%20Age-%20From%20Realism%20to%20Globalization%20%282004%29.pdf?forcedownload=1

Sampieri, R. (2014). Metodología de la Investigación. Recuperado de http://www.pucesi.edu.ec/webs/wp-content/uploads/2018/03/Hern%C3%A1ndez-Sampieri-R.-Fern%C3%A1ndez-Collado-C.-y-Baptista-Lucio-P.-2003.-Metodolog%C3%ADa-de-la-investigaci%C3%B3n.-M%C3%A9xico-McGraw-Hill-PDF.-Descarga-en-l%C3%ADnea.pdf

Viotti, P., Kauppi, M. (2012). International Relations Theory. Recuperado de https://www.pearson.com/us/higher-education/program/Viotti-International-Relations-Theory-5th-Edition/PGM8033.html

**ANEXOS**

*Anexo 1. Análisis de contenido de la rueda de prensa entre El Secretario de Defensa Robert Gates y el Jefe de Gabinete Mike Mullen sobre la revelación de documentos clasificados de Guerra por WikiLeaks*

| | | |
|---|---|---|
| Titulo | WikiLeaks revela documentos clasificados de Guerra | |
| Intervención | El Secretario de Defensa Robert Gates y el Jefe de Gabinete Mike Mullen | |
| Fecha de publicación | 29 de Julio 2010 | |
| Emisor | The White House | |
| Texto transcripto | Códigos preliminares | Códigos Finales |
| SEC. GATES: Good afternoon. I would first like to start with some comments about the release and subsequent publication of classified military documents earlier this week.<br><br>First, as the president stated, the problems identified and the issues raised in these documents relating to the war in Afghanistan have been well known in and out of government for some time. In fact, it was the recognition of many of these challenges that led to the president to conduct an extensive review of our Afghan strategy last year, which **concluded that our mission there needed a fundamentally new approach.** | Crear un nuevo enfoque para la guerra | Efectos disruptivos |
| These documents represent a mountain of raw data and individual impressions, most several years old, devoid of context or analysis. They do not represent official positions or policy. And they do not, in my view, fundamentally call into question the efficacy of our current strategy in Afghanistan and its prospects for success. Having said all that, the battlefield consequences of the **release of these documents are potentially severe and dangerous for our troops, our allies and Afghan partners, and may well damage our relationships and reputation in that key part of the world. Our adversaries will know** | Perjuicios en la imagen de EE.UU en otros lugares del mundo | Prestigio internacional |

| | | |
|---|---|---|
| **intelligence sources and methods, as well as military tactics, techniques and procedures.** | | |
| This department is conducting a thorough, aggressive investigation to determine how this leak occurred, to identify the person or persons responsible, and to assess the content of the information compromised. **We have a moral responsibility to do everything possible to mitigate the consequences for our troops and our partners downrange**, especially those who have worked with and put their trust in us in the past, who now may be targeted for retribution. | Mitigar efectos | Proteger la seguridad nacional |
| Yesterday, I called FBI Director Robert Mueller and asked for the FBI's assistance in our investigation as a partner. **It is important that we have all the resources we need to investigate and assess this breach of national security.** Furthermore, **the department is taking action in theater to prevent a repeat of such a breach, to include tightening procedures for accessing and transporting classified information.** | Evitar que sucedan violaciones a la seguridad nacional | Afectaciones a la Seguridad Nacional |
| As a general proposition, we endeavor to push access to sensitive battlefield information down to where it is most useful -- on the front lines -- where as a practical matter there are fewer restrictions and controls than at rear headquarters**. In the wake of this incident, it will be a real challenge to strike the right balance between security and providing our frontline troops the information they need.** | Información clasificada | Seguridad y protección de información |
| The U.S. military's success over the years rests on the abilities and integrity of its men and women in uniform and our trust in them. This trust is represented by the fact that, relative to other countries' armed forces, **our military culture is one that on the battlefield places great** | | |

| | | |
|---|---|---|
| **responsibility on the shoulders of even junior servicemembers, to include entrusting them with sensitive information.** The American way of war depends upon it. | Información clasificada | Seguridad y protección de información |
| But to earn and maintain that trust, we must all be responsible in handling, protecting and safeguarding our nation's secrets. For years there has been what I would call appropriate criticism of excessive classification and over classification of information. However, **this recent release of documents is a pointed reminder that much secret information is treated as such to protect sources of information**, to protect the lives of our men and women in uniform, to **deny our enemies the information about our military operations, and to preserve our relationships with friends and allies.**<br><br>This **recent massive breach should be a reminder to all entrusted with our secrets that there are potentially dramatic and grievously harmful consequences** of violations of trust and responsibility. We will aggressively investigate and, wherever possible, prosecute such violations. | Información secreta para mantener relaciones con aliados y prevenir ataques de enemigos | Seguridad y protección de información |
| ADM. MULLEN:<br><br>Thank you, Mr. Secretary. I certainly share your concerns about the recklessness with which classified documents were both leaked and then posted online.<br><br>As I said earlier this week, I am appalled by this behavior, and, frankly, outraged that anyone in their right mind would think it valuable to make public even one sensitive report, let alone tens of thousands of them, about a war that is being waged.<br><br>Yes, the documents are old and essentially raw inputs to our intelligence | | |

| | | |
|---|---|---|
| and operations apparatus. And yes, much of what has been revealed has already been commonly understood by the public or otherwise covered in the media. I can assure you, having just come from visits to Afghanistan and Pakistan, that none of what **I've seen posted online or reported in the press affects our overarching strategy.** | Efectos no nocivos en las estrategias estadounidenses | Filtración de información confidencial |
| But, frankly, that's not why this is so destructive. The sheer size and scope of the collection now **demands a careful review to determine the degree to which future tactical operations may be impacted**, and the degree to which the lives of our troops and Afghan partners may be at risk. And I think we always need to be mindful of the unknown potential for damage in any particular document that we handle.<br><br>Mr. Assange can say whatever he likes about the greater good he thinks he and his source are doing, but the truth is they might already have on their hands the blood of some young soldier or that of an Afghan family. Disagree with the war all you want, take issue with the policy, challenge me or our ground commanders on the decisions we make to accomplish the mission we've been given, but don't put those who willingly go into harm's way even further in harm's way just to satisfy your need to make a point. | Revisión para encontrar impactos en las operaciones de EE. UU | Afectaciones a las estrategias de EE. UU |
| Q Mr. Secretary, do you believe that the investigation should go beyond the source or sources of the leak within the military to include those who received or used the information -- WikiLeaks, the news media? And does the presence of the FBI in the investigation indicate such a widening of its scope?<br><br>SEC. GATES: Obviously, in the middle of an investigation, and particularly one that is in the military justice system, there's very little that I can say because of the potential for command influence. | | |

| | | |
|---|---|---|
| My basic position, though, is the **investigation should go wherever it needs to go.** And one of the reasons that I asked the director of the FBI to partner with us in this is to ensure that it can go wherever it needs to go. | Investigación profunda sobre el origen de la filtración y sus involucrados | Filtración de información confidencial |
| Q Admiral Mullen, you have mentioned that the founder of WikiLeaks may have blood on his hands. Do you know, have people been killed over this information?<br><br>ADM. MULLEN: They're still -- what I am concerned about with this is I think individuals who are not involved in this kind of warfare and expose this kind of information can't -- from my perspective, can't appreciate how **this kind of information is routinely networked together inside the classified channels we use specifically.**<br><br>And **it's very difficult, if you don't do this and understand this, to understand the impact, and very specifically the potential that is there** -- that is there to risk lives of our soldiers and sailors, airmen and Marines, coalition warfighters, as well -- as well as Afghan citizens. And there's no doubt in my mind about that.<br><br>SEC. GATES: I would just add one other thing. The thing to remember here is that this is a huge amount of raw data, as I said at the outset of my remarks. There is no accountability. There is no sense of responsibility. It is sort of thrown out there for take as you will and damn the consequences. | La información mal manejada por WL puede poner en riesgo vidas. | Riesgos de la filtración de información |

Fuente: The White House, 2010
Elaborado por: Torres, P. (2020)

*Anexo 2. Análisis de contenido de documentos sobre los esfuerzos de mitigación del gobierno de EE. UU. A la luz de la reciente divulgación ilegal de información clasificada por WikiLeaks*

| Titulo | FACT SHEET: U.S. Government Mitigation Efforts in Light of the Recent Unlawful Disclosure of Classified Information | |
|---|---|---|
| Intervención | Office of the Press Secretary | |
| Fecha de publicación | 01 diciembre 2010 | |
| Emisor | The White House | |
| Texto transcripto | Códigos preliminares | Códigos Finales |
| As part of an integrated federal government approach to respond to the unlawful and irresponsible disclosure of classified information by Wikileaks, **the National Security Staff has been coordinating an interagency effort to examine the policies and practices surrounding the handling of classified information, and to put in place safeguards to prevent such a compromise from happening again.**<br><br>The 9/11 attacks and their aftermath revealed gaps in intra-governmental information sharing. During the past decade, departments and agencies have tried to eliminate those gaps, resulting in considerable improvement in information-sharing. At the same time, federal policies underscore the importance of the existing prohibitions, restrictions, and requirements regarding the safeguarding of classified information. Our national security requires that sensitive information be maintained in confidence to protect our citizens, our democratic institutions, our homeland and our partners. Protecting information critical to our nation's security is the responsibility of each individual and agency granted access to classified information.<br><br>NATIONAL SECURITY STAFF INITIATIVES<br><br>On December 1, 2010, the National Security Advisor named Russell | Coordinación entre agencias para examinar las políticas y prácticas sobre el manejo de información clasificada, e implementar medidas para evitar que vuelva a ocurrir. | Seguridad y protección de Información |

| | | |
|---|---|---|
| Travers to serve as the National Security Staff's **Senior Advisor for Information Access and Security Policy**. **Travers will lead a comprehensive effort to identify and develop the structural reforms needed in light of the Wikileaks breach**. His responsibilities will include:<br><br>• Advising the National Security Staff on corrective actions, mitigation measures, and policy recommendations related to the breach.<br>• Facilitating interagency discussions and developing options for Deputies, Principals, and the President regarding technological and/or policy changes to limit the likelihood of such a leak reoccurring.<br>Additionally, **the President's Intelligence Advisory Board (PIAB) will take an independent look at the means by which the Executive Branch as a whole shares and protects classified information.** While the PIAB's traditional mandate is the examination of intelligence issues, the members' requisite security clearances, deep understanding of the wider United States Government national security mission and appreciation of the scope and complexity of classified government computer networks, make it particularly well-suited to immediately undertake this U.S. Government-wide review.<br>As a part of this undertaking, the PIAB will:<br><br>• Work with departments and agencies across the government to ensure they gain a comprehensive appreciation of all relevant challenges and requirements necessary to safeguard classified information and networks. | Nombramiento de Asesor Principal del Personal de Seguridad Nacional para el Acceso a la Información y la Política de Seguridad.<br><br>Desarrollar reformas estructurales necesarias debido a la divulgación de WikiLeaks<br><br>Revisión a todo el gobierno entorno a como comparte y protege información confidencial | Nuevo personal del gobierno enfocado en ciberseguridad<br><br>Reformas y revisiones en políticas sobre protección y seguridad de infraestructuras críticas de información<br><br>Reformas y revisiones en políticas sobre protección y seguridad de infraestructuras críticas de información |

| | | |
|---|---|---|
| • Examine the current posture of the whole of government with regard to leaks of classified information.<br>• Examine the balance between the need to share information and the need to protect information.<br>• Review the degree to which the government is organized to achieve information handling goals, consistent with our interests in security, information sharing, and transparency.<br><br>These efforts by the NSS and the PIAB will complement actions being taken across the Federal Government. The Office of Management and Budget (OMB**) has directed each department or agency that handles classified information establish a security assessment team consisting of counterintelligence, security, and information assurance experts to review the agency's implementation of procedures for safeguarding classified information against improper disclosures.** The OMB has directed that each review should include (without limitation) evaluation of the agency's configuration of classified government systems to ensure that users do not have broader access than is necessary to do their jobs effectively, as well as implementation of restrictions on usage of, and removable media capabilities from, classified government computer networks. **The OMB, the Information Security Oversight Office, and the Office of the Director of National Intelligence will stand up processes to evaluate, and to assist agencies in their review of security practices with respect to the protection of classified information.**<br><br>Prior to the issuance of this OMB Directive, **several agencies had proactively initiated measures to further safeguard classified** | Formación de equipos de evaluación de seguridad por expertos en contrainteligencia, seguridad y aseguramiento de la información.<br><br>Medidas para mitigar efectos de publicaciones y salvaguardar información de redes clasificadas | Especialistas en ciberseguridad para evaluar riesgos y amenazas cibernéticas<br><br>Reformas y revisiones en políticas sobre protección y seguridad de infraestructuras críticas de información |

| | | |
|---|---|---|
| **information and networks**. The following are examples of the numerous mitigation efforts underway across the interagency. | | |
| DEPARTMENT OF STATE INITIATIVES<br><br>The Secretary of State has commissioned a **review of State Department security procedures.** The Under Secretary for Management has assembled a team of senior management professionals in all related areas to **conduct a thorough review of current policies and procedures to ensure that they are fully abreast of the challenges faced.** Their efforts will be coordinated with the Bureau of Intelligence and Research to ensure that a measures taken strike the correct balance between **the critical need to protect classified information and the equally compelling requirement to ensure that it is shared with those who need it in their work to advance our national security.**<br><br>This review has already reaffirmed the Department's policy of deploying "thin client" computer units without removable media options and limiting the ability to download material from classified terminals to only approved and controlled circumstances.<br><br>The **Department will also deploy an automated tool that will continuously monitor the classified network to detect anomalies that would not be readily apparent.** This capability will be backed up by a professional staff who will promptly analyze these anomalies to ensure that they do not represent threats to the system.<br><br>The mandatory annual training and recertification requirement that all employees must satisfy is being | Revisión exhaustiva de los procedimientos y políticas de seguridad<br><br>Necesidad crítica de proteger la información y hacer buen uso de esta<br><br>Herramientas tecnológicas de ciberseguridad para proteger las redes de información | Revisión de las prácticas de seguridad<br><br>Reformas y revisiones en políticas sobre protección y seguridad de infraestructuras críticas de información<br><br>Ciberseguridad para proteger información de intrusos externos |

| | | |
|---|---|---|
| reviewed to see if additional material needs to be added to bolster this on-going effort.<br><br>In the interim, the Department has suspended access to the Net Centric Diplomacy (NCD) database of diplomatic reporting , and its classified "ClassNet" web sites and SharePoint sites previously accessible through the Secret Internet Protocol Router Network (SIPRNet), while retaining access via the Joint Worldwide Intelligence Communications System | | |
| DEPARTMENT OF DEFENSE (DoD) INITIATIVES<br><br>On August 12, 2010, Defense Secretary Robert Gates commissioned **two reviews to determine what policy, procedural and/or technological shortfalls contributed to the unauthorized disclosure to the Wikileaks website**. He specifically directed an assessment to determine if the DoD had appropriately balanced restrictions associated with information security and the need to provide our front-line personnel with the information needed to accomplish their assigned missions.<br><br>As a result of these two reviews, a number of findings and **recommendations are in the process of being assessed and implemented, including the following**:<br><br>• Disabling and controlling use of removable storage media on DoD classified networks to prevent download from classified networks.<br>• Developing procedures to monitor and detect suspicious, unusual or anomalous user behavior (similar to procedures now being implemented by credit card companies to detect and monitor fraud). | Revisiones para encontrar las fallas que contribuyeron a la divulgación de información de WikiLeaks<br><br>Medidas de seguridad necesarias<br><br>Desarrollo de herramientas tecnológicas para monitorear y detectar movimientos sospechosos | Encontrar vulnerabilidades y fallas en las redes del gobierno<br><br>Reformas, revisiones y pruebas sobre los procesos de manejo de información |

| | | |
|---|---|---|
| • Conducting security oversight inspections in all Combatant Commands.<br>• Undertaking vulnerability assessments of DoD networks.<br>• **Improving awareness and compliance with information protection procedures**. Specific examples being undertaken at the Combatant Command level include:<br>• Increased "insider threat" training focusing on awareness of associated activity.<br>• Multi-discipline training between traditional security, law enforcement and information assurance at all echelons.<br>• **The establishment of "Insider Threat Working Groups" to address the Wikileaks incident and prevent reoccurrence.**<br>• **Component-determined restricted access to the Wikileaks site to prevent further dissemination or downloading of classified information to unclassified DoD networks.**<br>• Restating of policy to all personnel regarding restrictions on downloading to government systems and cautionary advice regarding personal IT systems.<br><br>Individual DoD components are taking additional action as relevant and appropriate, ranging from random physical inspections **to enabling new security features on networks**. Leadership reinforcement of workforce responsibilities **and new initiatives to safeguard information are key components of DoD's mitigation efforts**. Department-wide, **the Pentagon is accelerating its publication of policy issuances related to the information security program** as well as focusing increased attention on detecting **potential insider threats.** | Evaluaciones para ver la vulnerabilidad de las redes<br><br>Grupos de trabajo sobre amenazas internas en el caso de WikiLeaks<br><br>Aumentar seguridad en los sistemas informáticos que restrinjan el acceso a WikiLeaks<br><br>Nuevas funciones de seguridad en las redes<br><br>Incrementar la detención de amenazas internas | confidencial en las redes del gobierno<br><br>Especialistas en ciberseguridad para evaluar riesgos y amenazas cibernéticas<br><br>Ciberseguridad para proteger información de intrusos externos<br><br>Innovación tecnológica en ciberseguridad<br><br>Políticas, estrategias, programas y |

| | | |
|---|---|---|
| OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE (ODNI) INITIATIVES<br><br>The ODNI is working as part of the integrated whole of government approach to **assist agencies in their review of security practices**.<br><br>In coordination with the larger OMB effort, ODNI is developing recommendations to enhance security within the Intelligence Community (IC), to include:<br><br>• Insider Threat Assessment Inspections: Departments and Agencies will establish inspection teams, with assistance provided by ODNI/ONCIX, consisting of Counterintelligence (CI), **Security, and Information Assurance** (IA) experts to identify removable media policies and their implementation.<br>• **Enhanced Automated, On-Line Audit Capability**: Systems will monitor user activity on all IC classified computer systems to detect unusual behavior. Additionally, a fully staffed analytic capability will put a human eye on the suspect activity.<br>• Removable Media Policies Review: Department and Agencies will review current policies and procedures to reduce risk posed by removable media within each organization. | Asistir a las agencias en las revisiones de seguridad<br><br>Equipos de inspección de amenazas internas<br><br>Uso de tecnología de ciberseguridad | leyes de ciberseguridad<br><br>Revisión de las prácticas de seguridad<br><br>Especialistas en ciberseguridad para evaluar riesgos y amenazas cibernéticas<br><br>Innovación tecnológica en ciberseguridad |

| | | |
|---|---|---|
| • Policy Compliance Action Plan: Departments and Agencies will assess the level of compliance with existing CI, Security, and IA policies to identify discrepancies and will establish a plan to track and report improvements.<br>• **Information Assurance Training**: Departments and Agencies will conduct mandatory regular trainings for all employees on the handling of classified information.<br>• Review Secure Device Settings: Departments and Agencies will mandate a compliance review of secure system configuration settings. | Capacitaciones al personal para mejorar la protección de información clasificada | Concientización sobre la importancia de la ciberseguridad |

Fuente: The White House, Office of the Press Secretary, 2010
Elaborado por: Torres, P. (2020)

*Anexo 3. Análisis de contenido de las declaraciones del Subsecretario de Defensa sobre las divulgaciones de WikiLeaks*

| Titulo | Publicaciones de WikiLeaks | |
|---|---|---|
| Intervención | Whitman, Bryan Mr OSD PA | |
| Fecha de publicación | 28 de Noviembre 2010 | |
| Emisor | U.S. Department of Defense Office of the Assistant Secretary of Defense (Public Affairs) | |
| Texto transcripto | Códigos preliminares | Códigos Finales |
| As you may be aware, several news organizations are about to publish stories on hundreds of thousands of stolen classified State Department documents provided to them by WikiLeaks. As we have in the past, **we condemn this reckless disclosure of classified information illegally obtained.**<br><br>We also want to provide you with context and details regarding ongoing | Rechazo total a las divulgaciones de WikiLeaks | Filtración de información confidencial |

| | | |
|---|---|---|
| efforts to prevent further compromise of sensitive data.<br><br>The 9/11 attacks and their aftermath revealed gaps in intra-governmental information sharing. Departments and agencies have taken significant steps to reduce those obstacles, and the work that has been done to date has resulted in considerable improvement in information-sharing and increased cooperation across government operations.<br><br>However, as we have now seen with the theft of huge amounts of classified data and the Wikileaks compromises, **these efforts to give diplomatic, military, law enforcement and intelligence specialists quicker and easier access to greater amounts of data have had unintended consequences making our sensitive data more vulnerable to compromise.**<br><br>That said, the Department has undertaken a series of actions to prevent such incidents from occurring in the future. | Cambios realizados para el manejo de información también han causado vulnerabilidad | Seguridad y protección de información |
| On August 12, 2010, Defense Secretary Robert Gates commissioned two reviews to determine what policy, procedural and/or technological shortfalls contributed to the unauthorized disclosure to the Wikileaks website.<br><br>As a result of these two reviews, a number of findings and recommendations are in the process of being reviewed and implemented, including the following:<br><br>Directing actions to include disabling all write capability to removable media on DoD classified computers, as a temporary **technical solution to mitigate the future risks of personnel** | Evitar el traslado de información clasificada | Revisión de las prácticas de seguridad |

| | | |
|---|---|---|
| **moving classified data to unclassified systems.**<br><br>Directing DoD organizations to have limited number of systems authorized to move data from classified to unclassified systems (**similar to a KIOSK concept, where it is necessary to meet at a central, supervised location to conduct this activity).**<br><br>• Directing DoD organizations to implement two-person handling rules for moving data from classified to unclassified systems to ensure proper oversight and reduce chances of unauthorized release of classified material.<br>• Developing procedures to monitor and detect suspicious, unusual or anomalous user behavior (similar to procedures now being used by credit card companies to detect and monitor fraud).<br>• **60% of DoDs SIPR-net is now equipped with HBSS (Host-Based Security System)** an automated way of controlling the computer system with a capability of monitoring unusual data access or usage. DoD is accelerating HBSS deployment to its SIPR-net systems.<br><br>Conducting security oversight inspections in forward-deployed areas.<br>Undertaking vulnerability assessments of DoD networks.<br><br>Improving awareness and compliance with information protection procedures. For example, CENTCOM has:<br><br>• Increased insider threat training focusing on awareness of associated activity.<br>• **Initiated multi-discipline training between traditional security, law enforcement and** | Implementar procesos y reglas de seguridad para mover información<br><br>Implementación de nuevo sistema de ciberseguridad para controlar movimientos inusuales<br><br>Refuerzo y aplicación de leyes de seguridad para asegurar la información | Reformas y revisiones en políticas sobre protección y seguridad de infraestructuras críticas de información<br><br>Innovación tecnológica en ciberseguridad<br><br>Políticas, estrategias, programas y leyes de ciberseguridad |

| | | |
|---|---|---|
| **information assurance at all echelons**.<br>• Established "Insider Threat Working Groups" to address the WIkileaks incident and prevent reoccurrence.<br>• Informed all personnel of restrictions on downloading to government systems and cautioned regarding personal IT systems.<br>• Bottom line: **It is now much more difficult for a determined actor to get access to and move information outside of authorized channels.**<br><br>Regards,<br><br>Bryan Whitman | Estas precauciones han aumentado la dificultad de acceder a las redes privadas de EE.UUs | Seguridad y protección de información |

Fuente: U.S. Department of Defense, 2010
Elaborado por: Torres, P. (2020)

*Anexo. 4 Análisis de contenido del lanzamiento de la estrategia Internacional para el Ciberespacio por Howard Schmidt*

| Titulo | Launching the U.S. International Strategy for Cyberspace | |
|---|---|---|
| Intervención | Howard Schmidt | |
| Fecha de publicación | 16 de Mayo del 2011 | |
| Emisor | The White House | |
| Texto transcripto | Códigos preliminares | Códigos finales |
| Today, I am proud to announce the United States' first, comprehensive International Strategy for Cyberspace (pdf). The International Strategy is a historic policy document for the 21st Century — one that explains, for audiences at home and abroad, **what the U.S. stands for internationally in cyberspace, and how we plan to build prosperity, enhance security, and safeguard openness in our increasingly networked world.**<br><br>Today, Homeland Security Advisor John Brennan and I were joined by Secretary | Explicar a nivel nacional e internacional las mejoras que se necesitan para implementar seguridad para operar en el ciberespacio | Liderazgo en el ciberespacio |

| | | |
|---|---|---|
| of State Hillary Clinton, Attorney General Eric Holder, Secretary of Commerce Gary Locke, Secretary of Homeland Security Janet Napolitano and Deputy Secretary of Defense Bill Lynn in announcing this landmark document's release, here at the White House. The event was streamed live on WhiteHouse.gov, and you can view it here starting this evening. | | |
| The International Strategy lays out the President's **vision for the future of the Internet, and sets an agenda for partnering with other nations and peoples to achieve that vision**. It begins by recognizing the successes networked technologies have brought us, in large part due to the spirit of freedom and innovation that has characterized the Internet from its early days as a research project. While the strategy is realistic about the challenges we face, it nonetheless emphasizes that our policies must continue to be grounded in our core principles of fundamental freedoms, privacy, and the free flow of information. | Iniciativas para el futuro del internet con el apoyo de otros países | Liderazgo en el ciberespacio |
| To achieve our vision, the United States will build an international environment that ensures global networks are open to new innovations, interoperable the world over, secure enough to support people's work, and reliable enough to earn their trust. **To achieve it, we will build and sustain an environment in which norms of responsible behavior guide states' actions, sustain partnerships, and support the rule of law**. | Crear un entorno con normas para controlar el ciberespacio | Liderazgo en el ciberespacio |
| **The International Strategy is larger than any one department or agency. It is a strong foundation for the diverse activities we will carry out across our entire government**. It is about the principles that unite our nation, the vision that unites our policy, and the **priorities that unite our government.** | La seguridad en el ciberespacio es una prioridad del gobierno | Protección de la nación en el ciberespacio |

| | | |
|---|---|---|
| With our partners around the world, we will work to create a **future for cyberspace that builds prosperity, enhances security, and safeguards openness in our networked world**. This is the future we seek, and we invite all nations, and peoples, to join us in that effort. | | |

Fuente: The White House, 2011
Elaborado por: Torres, P. (2020)

*Anexo. 5 Análisis de contenido del segmento de la Introducción por Barack Obama de la Estrategia Internacional para el Ciberespacio*

| Titulo | Estrategia Internacional para el Ciberespacio | |
|---|---|---|
| Intervención | Introducción de Barack Obama | |
| Fecha de publicación | Mayo 2011 | |
| Emisor | The White House | |
| Texto transcripto | Códigos preliminares | Códigos finales |
| Cyberspace, and the technologies that enable it, allow people of every nationality, race, faith, and point of view to communicate, cooperate, and prosper like never before. Today, an American company can do business anywhere in the world with an Internet connection, supporting countless jobs and opportunities for the American people. A mother in rural Africa can sell crafts to a family in Latin America, advancing broader economic development. A laboratory in Europe can conduct fieldchanging research on hardware made in Asia and software written in North America, and students in Australia and the Middle East can learn together through videoconference. And more than ever, citizens across the globe are being **empowered with information technologies to help make their governments more open and responsive.** | Interconectividad mundial gracias a las tecnologías de la comunicación | Globalización |
| Today, as nations and peoples harness the networks that are all around us, we have a choice. We can either work together to realize their potential for greater prosperity and security, or we | | |

| | | |
|---|---|---|
| can succumb to narrow interests and undue fears that limit progress. **Cybersecurity is not an end unto itself; it is instead an obligation that our governments and societies must take on willingly, to ensure that innovation continues to flourish, drive markets, and improve lives.** While offline challenges of crime and aggression have made their way to the digital world, we will confront them consistent with the principles we hold dear: free speech and association, privacy, and the free flow of information. | Implementar Ciberseguridad es una obligación importante de prioridad nacional | Proteger la seguridad nacional |
| The digital world is no longer a lawless frontier, nor the province of a small elite. It is a place where the norms of responsible, just, and peaceful conduct among states and peoples have begun to take hold. It is one of the finest examples of a community self-organizing, as civil society, academia, the private sector, and governments work together democratically to ensure its effective management. **Most important of all, this space continues to grow, develop, and promote prosperity, security, and openness** as it has since its invention. This is what sets the Internet apart in the international environment, and why it is so important to protect. In this spirit, I offer the United States' International Strategy for Cyberspace. | Ciberespacio sigue en constante desarrollo para aumentar la protección de este espacio esta Estrategia ofrece las bases | Innovación tecnológica en ciberseguridad |
| This is not the first time my Administration has addressed the policy challenges surrounding these technologies, **but it is the first time that our Nation has laid out an approach that unifies our engagement with international partners on the full range of cyber issues**. And so this strategy outlines not only a vision for the future of cyberspace, but an agenda for realizing it. It provides the context for our partners at home and **abroad to understand our priorities, and how we can come together to preserve the** | Iniciativa internacional para resolver problemas cibernéticos en conjunto | Prestigio internacional |

| | | |
|---|---|---|
| **character of cyberspace and reduce the threats we face**. By itself, the Internet will not usher in a new era of international cooperation. That work is up to us, its beneficiaries. Together, we can work together to build a future for **cyberspace that is open, interoperable, secure, and reliable**. This is the future we seek, and we invite all nations, and peoples, to join us in that effort | | |

Fuente: The White House, 2011
Elaborado por: Torres, P. (2020)

*Anexo. 6 Análisis de contenido del lanzamiento de la Blueprint for a Secure Cyber Future por la secretaria del Departamento de Estado Jannet Napoliano*

| Titulo | Lanzamiento de la estrategia Blueprint for a Secure Cyber Future | |
|---|---|---|
| Intervención | Secretaria del Departamento de Estado Jannet Napoliano | |
| Fecha de publicación | Noviembre 2011 | |
| Emisor | Department of Homeland Security | |
| Texto transcripto | Códigos preliminares | Códigos finales |
| I am pleased to release the Blueprint for a Secure Cyber Future: The Cybersecurity Strategy for the Homeland Security Enterprise. This strategy was developed pursuant to the Department of Homeland Security (DHS) Quadrennial Homeland Security Review and **reflects the importance of cyberspace to our economy, security, and way of life. This strategy provides a blueprint for a cyberspace that enables innovation and prosperity, advances our economic interests and national security, and integrates privacy and civil liberties protections into the Department's cybersecurity activities.** The strategy **is designed to protect the critical systems and assets that are vital to the United States**, and, over time, to foster stronger, more resilient information and communication technologies to enable government, business and individuals to be safer online. | Protección de sistemas críticos de EE. UU incrementar tecnologías de información y comunicación más fuertes y resistentes | Innovación tecnológica en ciberseguridad |

| | | |
|---|---|---|
| Cybersecurity is a shared responsibility, and each of us has a role to **play. Emerging cyber threats require the engagement of the entire society—from government and law enforcement to the private sector and most importantly, members of the public.** Today in cyberspace, **the Nation faces a myriad of threats from criminals, including individual hackers and organized criminal groups, as well as technologically advanced nation-states. Individuals and well-organized groups exploit technical vulnerabilities to steal American intellectual property, personal information, and financial data.** The increasing number and sophistication of these incidents has the potential to impact our economic competitiveness and threaten the public's ability to access and obtain basic services. Government, non-governmental and private sector entities, as well as individuals, families, and communities must collaborate on ways to effectively reduce risk. In preparing the strategy, the Department benefited from the constructive engagement of representatives from state and local governments, industry, academia, non-governmental organizations, and many dedicated individuals from across the country. | Crecientes amenazas cibernéticas atacan e impactan al crecimiento económico y seguridad<br><br>Amenazas de grupos criminales e individuos que encuentran vulnerabilidades técnicas del gobierno y roban información | Amenazas cibernéticas<br><br>Hackers |
| We appreciate that support. **DHS also worked closely with federal departments and agencies to refine the strategy and ensure consistency with the President's 2010 National Security Strategy**, the Department of Defense Strategy for Operating in Cyberspace, and the President's International Strategy for Cyberspace. I want to acknowledge the efforts and commitment of the men and women of DHS and the many thousands of computer scientists, systems engineers, law enforcement personnel, and other | Departamentos y agencias trabajando en conjunto en temas se ciberseguridad | Reformas y revisiones en políticas sobre protección y seguridad de infraestructuras críticas de información |

| | | |
|---|---|---|
| professionals across the country who work tirelessly to safeguard and secure cyberspace. On their behalf, I am pleased to release this Blueprint for a Secure Cyber Future. | | |

Fuente: Department of Homeland Security, 2011
Elaborado por: Torres, P. (2020)

*Anexo 7. Análisis de contenido de la hoja de trabajo de la estrategia Blueprint for a secure cyber future*

| Titulo | Hoja de trabajo de la estrategia Blueprint for a Secure Cyber Future | |
|---|---|---|
| Fecha de publicación | 12 de diciembre 2011 | |
| Emisor | Department of Homeland Security | |
| Texto transcripto | Códigos preliminares | Códigos finales |
| **The United States is facing a continued and growing cyber threat, which has the potential to jeopardize our national security, public safety and economic competitiveness. This threat makes securing cyberspace one of the most important missions facing** the homeland security community today. | Amenazas cibernéticas constantes que ponen en peligro la seguridad nacional y el crecimiento económico<br>Prioridad aumentar seguridad en el ciberespacio | Protección de la nación en el ciberespacio |
| The Department of **Homeland Security's 2010 Quadrennial Homeland Security Review (QHSR) established the safeguarding and securing of cyberspace as a critical mission of DHS**, with the goals to create a safe, secure and resilient cyber environment and promote cybersecurity knowledge and innovation. The Blueprint proposes a path forward to achieve these goals. | Protegerse en el ciberespacio es una misión crítica | Ciberespacio nuevo dominio de poder |
| The *Blueprint* calls for a coordinated effort across the homeland security community to protect our nation's **critical information infrastructure and build a safer and more secure cyber ecosystem**. **Specific actions range from hardening critical networks and prosecuting cybercrime to raising public** | Lograr un ecosistema cibernético más seguro que consiste en fortalecer las redes críticas, enjuiciar el delito cibernético, aumentar la conciencia pública y crear una fuerza laboral nacional de seguridad cibernética. | Fortalecimiento en todo aspecto de la Ciberseguridad |

| | | |
|---|---|---|
| **awareness and training a national cybersecurity workforce.**<br><br>**Cyberspace forms the backbone of our modern economy and society**. The Internet is an engine of immense wealth creation and a force for openness, transparency, innovation, and freedom. Information and communication technologies allow generators to turn, businesses to operate, and families and friends to communicate. **Cyberspace is vital to our way of life, and we must work to make this domain more secure—the safety of our critical infrastructure, the strength of our national security, our economic vitality and public safety depend upon it.**<br><br>The Blueprint outlines an integrated and holistic approach to protecting our nation's cyberspace. It is a map – a guide – to enable the homeland security community to leverage existing capabilities and promote technological advances that enable government, the private sector and the public to be safer online. | Dependencia al ciberespacio, obligación de hacer este dominio más seguro para fortalecer la seguridad nacional | Ciberpoder |
| The document complements the President's International Strategy for Cyberspace, the National Strategy for Trusted Identities in Cyberspace and the recently released Department of Defense Strategy for Operating in Cyberspace. Together, these documents provide a **whole of government approach to the many opportunities and challenges the nation faces in cyberspace**.<br><br>Cybersecurity is a shared responsibility, and each of us has a role to play. DHS will work with federal, state, local and private sector partners across the homeland security community to achieve the goals outlined in the *Blueprint*. Implementing the Blueprint will be an inclusive, | Enfoque para disminuir peligros en el ciberespacio para que EE. UU prosperé sin inconvenientes | Ciberpoder |

| | | |
|---|---|---|
| participatory **effort to make cyberspace a safe, secure and resilient place where the American way of life can thrive.** | | |

Fuente: Department of Homeland Security, 2011
Elaborado por: Torres, P. (2020)

*Anexo. 8 Análisis de contenido del discurso de lanzamiento de la Estrategia de Seguridad Nacional del 2010 por el consejero de seguridad nacional James L. Jones*

| Titulo | la Estrategia de Seguridad Nacional del 2010 | |
|---|---|---|
| Intervención | Consejero de Seguridad Nacional General James L. Jones | |
| Fecha de publicación | 27 de mayo 2010 | |
| Emisor | Departamento de Estado | |
| Texto transcripto | Códigos preliminares | Códigos finales |
| First, we must deal with the world as it is, and this strategy is guided by a clear-eyed understanding of our strategic environment, the world as it is today. This is a time of sweeping change. Two decades since the end of the Cold War, **the free flow of information, people and trade continues to accelerate at an unprecedented pace. Events far beyond our nation's shores now impact our safety, our security, and prosperity**, and that of our allies and friends alike in ways that we could not have imagined just a few years ago.<br><br>This interconnection comes with extraordinary promise and it reinforces many of our innate strengths, our openness, our diversity, our dynamism, our ingenuity, and our dedication to our goals and aspirations. **But this interconnection also comes with the perils of global challenges that do not respect borders – global networks of terrorists and criminals, threats in space and cyberspace, the degrading climate and technologies with increasing destructive power**. ---------- | Interconectividad constante transciende las fronteras geográficas lo que genera impacto en la seguridad y prosperidad de la nación<br><br>Nuevas redes de amenazas globales tecnológicas con poder destructivo | Globalización<br><br>Amenazas cibernéticas |

| | | |
|---|---|---|
| In addition, the international architecture of the 20th century, designed for another time, is buckling under the weight of these **new threats**. As a consequence, it has been difficult to forge the cooperative approach as necessary to prevent states from flouting international norms and agreements. This strategy recognizes the changes required in order to be **successful in the new environment of the 21st century**. And that is the world that we seek.<br><br>**This is the first National Security Strategy to highlight the importance of cyber security**. **It embraces the 21st century power dynamics** and the first deliberate strategy for building constructive ties with emerging centers of influence, including by elevating the role of the Governemnt as the focal point for international economic cooperation. And the core premise that the promotion of human rights and democracy are core national interests. We lead on behalf of those efforts, above all, through the power of our own example, as I mentioned earlier. | estrategia para operar en el nuevo entorno internacional del siglo 21 contra las "nuevas amenazas"<br><br>Resalta la importancia del ciberespacio y por lo tanto el desarrollo de ciberseguridad<br><br>Dinámica del poder del siglo 21 | Políticas, estrategias, programas y leyes de ciberseguridad<br><br>Concientización sobre la importancia de la ciberseguridad<br><br>Ciberpoder |

Fuente: Department of State, 2010
Elaborado por: Torres, P. (2020)

*Anexo 9. Análisis de contenido del Asistente del Presidente de Seguridad Nacional y Contraterrorismo - John Brennan sobre la presentación del nuevo coordinador de seguridad*

| Titulo | Introducción del Nuevo coordinador de ciberseguridad | |
|---|---|---|
| Intervención | Asistente del Presidente de Seguridad Nacional y Contraterrorismo - John Brennan | |
| Fecha de publicación | 22 de diciembre 2009 | |
| Emisor | The White House | |
| Texto transcripto | Códigos preliminares | Códigos |
| **Cybersecurity matters to all of us. Protecting the internet is critical to our national security**, public safety and our personal privacy and civil liberties. **It's also vital to President Obama's efforts to strengthen our country**, from the modernization of our | Ciberseguridad para proteger la seguridad nacional | Proteger la seguridad nacional |

| | | |
|---|---|---|
| health care system to the high-tech job creation central to our economic recovery.<br><br>The very email you are reading **underscores our dependence on information technologies in this digital age, which is why it seemed like a fitting way to announce that the President has chosen Howard Schmidt to be the White House Cybersecurity Coordinator**. Howard will have the important responsibility of orchestrating the many important cybersecurity activities across the government.<br><br>Howard is one of the world's leading authorities on computer security, with some 40 years of experience in government, business and law enforcement. Learn more about Howard's background and approach to cybersecurity.<br>**Howard will have regular access to the President and serve as a key member of his National Security Staff. He will also work closely with his economic team to ensure that our cybersecurity efforts keep the Nation secure and prosperous**.<br>Moving forward we will use WhiteHouse.gov, this email program and our other communications tools to keep you posted about our progress in this important area.<br>Sincerely,<br><br>John O. Brennan<br>Assistant to the President for Homeland Security and Counterterrorism | Dependencia a las tecnologías de información, necesidad de establecer a un nuevo Coordinador de ciberseguridad<br><br>Garantizar los esfuerzos en seguridad cibernética | Nuevo personal del gobierno enfocado en ciberseguridad<br><br>Mayor preparación en ciberseguridad |

Fuente: The White House, 2009
Elaborado por: Torres, P. (2020)

*Anexo. 10 Análisis de contenido sobre el anuncio de los planes para asegurar el futuro digital de Estados Unidos*

| | |
|---|---|
| Titulo | El presidente anuncia sus planes para asegurar el futuro digital de Estados Unidos |
| Intervención | Barack Obama |

| Fecha de publicación | 29 de Mayo 2009 | |
|---|---|---|
| Emisor | The White House | |
| Texto transcripto | Códigos preliminares | Códigos finales |
| We meet today at a transformational moment – a moment in history **when our interconnected world presents us, at once, with great promise but also great peril.** Now, over the past four months my administration **has taken decisive steps to seize the promise and confront these perils**. We're working to recover from a global recession while laying a new foundation for lasting prosperity. We're strengthening our armed forces as they fight two wars, at the same time **we're renewing American leadership to confront unconventional challenges**, from nuclear proliferation to terrorism, from climate change to pandemic disease.<br><br>And we're bringing to government and to this White House unprecedented transparency and accountability and new ways for Americans to participate in their democracy. But none of this progress would be possible, **and none of these 21st century challenges can be fully met, without America's digital infrastructure -- the backbone that underpins a prosperous economy and a strong military and an open and efficient government**. Without that foundation we can't get the job done. It's long been said that the revolutions in communications and information technology have given birth to a virtual world. But make no mistake: **This world cyberspace is a world that we depend on every single day.**<br><br>It's our hardware and our software, our desktops and laptops and cell phones and Blackberries that have become woven into every aspect of our lives. It's the broadband networks beneath us and the wireless signals around us, the local networks in our schools and hospitals and businesses, and the massive grids that power our nation. **It's the classified** | Medidas para afrontar los peligros que trae la interconectividad<br><br>Ampliar estrategias de poder para mantener el liderazgo<br><br>Aumentar capacidades tecnológicas por la dependencia al ciberespacio | Respuestas a incidentes cibernéticos<br><br>Liderazgo en el ciberespacio<br><br>Innovación tecnológica en ciberseguridad<br><br>Afectaciones a la Seguridad Nacional |

| | | |
|---|---|---|
| **military and intelligence networks that keep us safe, and the World Wide Web that has made us more interconnected than at any time in human history.So cyberspace is real and so are the risks that come with it.** | Riesgos del ciberespacio son reales | |
| It's the great irony of our Information Age **the very technologies that empower us to create and to build also empower those who would disrupt and destroy** and this paradox seen and unseen is something that we experience every day. It's about the privacy and the economic security of American families. We rely on the Internet to pay our bills, to bank, to shop, to file our taxes. But we've had to learn a whole new vocabulary just to stay ahead of the **cyber criminals who would do us harm** -- spyware and malware and spoofing and phishing and botnets. millions of Americans have been victimized, their privacy violated, their identities stolen, their lives upended, and their wallets emptied | Empoderamiento de diferentes actores para causar daños | Efectos disruptivos |
| According to one survey, in the past two years alone cyber crime has cost Americans more than $8 billion. I know how it feels to have privacy violated because it has happened to me and the people around me. It's no secret that my presidential campaign harnessed the Internet and technology to transform our politics. **What isn't widely known is that during the general election hackers managed to penetrate our computer systems**. to all of you who donated to our campaign, I want you to all rest assured, our fundraising website was untouched. So your confidential personal and financial information was protected but between August and October, **hackers gained access to emails and a range of campaign files, from policy position papers to travel plans and we worked closely with the CIA -- with the FBI and the Secret Service and hired security consultants** | Ataques de Hackers para robar información sensible | Hackers |

| | | |
|---|---|---|
| **to restore the security of our systems**. It was a powerful reminder: in this Information Age, one of your greatest strengths in our case, our ability to communicate to a wide range of supporters through the Internet could also be one of your greatest vulnerabilities.<br><br>This is a matter, as well, of America's economic competitiveness. the small businesswoman in St. Louis, the bond trader in the New York Stock Exchange, the workers at a global shipping company in Memphis, the young entrepreneur in Silicon Valley they all need the networks to make the next payroll, the next trade, the next delivery, the next great breakthrough. E-commerce alone last year accounted for some $132 billion in retail sales. But every day we see waves of **cyber thieves trolling for sensitive information** -- the disgruntled employee on the inside, the lone hacker a thousand miles away, organized crime, the industrial spy and, increasingly, foreign intelligence services. In one brazen act last year, thieves used stolen credit card information to steal millions of dollars from 130 ATM machines in 49 cities around the world and they did it in just 30 minutes. a single employee of an American company was convicted of stealing intellectual property reportedly worth $400 million. | Robo de información | Hackers |
| It's been estimated that last year alone cyber criminals stole intellectual property from businesses worldwide worth up to $1 trillion. In short, **America's economic prosperity in the 21st century will depend on cybersecurity. And this is also a matter of public safety and national security**. we count on computer networks to deliver our oil and gas, our power and our water. We rely on them for public transportation and air traffic control yet **we know that cyber** | Prosperidad y salvaguarda de la seguridad nacional depende de la ciberseguridad | Proteger la seguridad nacional<br><br>Ciberpoder |

| | | |
|---|---|---|
| **intruders have probed our electrical grid and that in other countries cyber attacks have plunged entire cities into darkness**.<br><br>**Our technological advantage is a key to America's military dominance but our defense and military networks are under constant attack**. Al Qaeda and other terrorist groups have spoken of their desire to unleash a **cyber attack on our country -- attacks that are harder to detect and harder to defend against**. Indeed, in today's world, acts of terror could come not only from a few extremists in suicide vests **but from a few key strokes on the compute**r -- a weapon of mass disruption. In one of the most serious cyber incidents to date against our military networks, several thousand computers were infected last year by malicious software -- malware. And while no sensitive information was compromised, our troops and defense personnel had to give up those external memory devices thumb drives changing the way they used their computers every day and last year **we had a glimpse of the future face of war.** | Capacidades tecnológicas son claves para el dominio de EE. UU<br><br>Ataques cibernéticos han cambiado las formas de hacer daños son una nueva arma de guerra | Ataques cibernéticos y acciones disruptivas |
| As Russian tanks rolled into Georgia, cyber attacks crippled Georgian government websites.The terrorists that sowed so much death and destruction in Mumbai relied not only on guns and grenades but also on GPS and phones using voice-over-the-Internet. For all these reasons, it's now clear this **cyber threat is one of the most serious economic and national security challenges we face as a nation.**<br><br>**It's also clear that we're not as prepared as we should be**, **as a government or as a country**. In recent years, some progress has been made at the federal level but just as we failed in the past to invest in our physical infrastructure -- our roads, our bridges and rails we've failed to invest in the | El ciberespacio trae los mayores desafíos para salvaguardar la economía y la seguridad nacional<br><br>Necesidad de mayor preparación en el ciberespacio | Amenazas cibernéticas<br><br>Políticas, estrategias, programas y leyes de ciberseguridad |

| | | |
|---|---|---|
| security of our digital infrastructure. **No single official oversees cybersecurity policy across the federal government, and no single agency has the responsibility or authority to match the scope and scale of the challenge**. Indeed, when it comes to cybersecurity, federal agencies have overlapping missions and don't coordinate and communicate nearly as well as they should with each other or with the private sector.<br><br>We saw this in the disorganized response to Conficker, the Internet "worm" that in recent months has infected millions of computers around the world. This status quo is no longer acceptable not when there's so much at stake. We can and we must do better and that's why shortly after taking **office I directed my National Security Council and Homeland Security Council to conduct a top-to-bottom review of the federal government's efforts to defend our information and communications infrastructure and to recommend the best way to ensure that these networks are able to secure our networks as well as our prosperity**. Our review was open and transparent. I want to acknowledge, Melissa Hathaway, who is here, who is the Acting Senior Director for Cyberspace on our National Security Council, who led the review team, as well as the Center for Strategic and International Studies bipartisan Commission on Cybersecurity, and all who were part of our 60-day review team. They listened to a wide variety of groups, many of which are represented here today and I want to thank for their input: industry and academia, civil liberties and private privacy advocates.<br><br>We listened to every level and branch of government from local to state to federal, civilian, military, homeland as | Revisión general del estado de ciberseguridad del país | Reformas y revisiones en políticas sobre protección y seguridad de infraestructuras críticas de información |

| | | |
|---|---|---|
| well as intelligence, Congress and international partners, as well.<br><br>I consulted with my national security teams, my homeland security teams, and my economic advisors. Today I'm releasing a report on our review and can announce that **my administration will pursue a new comprehensive approach to securing America's digital infrastructure. This new approach starts at the top, with this commitment from me: From now on, our digital infrastructure the networks and computers we depend on every day will be treated as they should be: as a strategic national asset. Protecting this infrastructure will be a national security priority.** | Infraestructura digital y redes consideradas como un activo nacional estratégico<br>Protección de estas infraestructuras es una prioridad del gobierno | Proteger la seguridad nacional |
| We will ensure that these networks are secure, trustworthy and resilient. **We will deter, prevent, detect, and defend against attacks and recover quickly from any disruptions or damage**. To give these efforts the high-level focus and attention they deserve and as part of the new, single National Security Staff announced this week. I'm creating a new office here at the White House that will be led by **the Cybersecurity Coordinator. Because of the critical importance of this work,**<br><br>I will personally select this official. I'll depend on this official in all matters relating to<br>cybersecurity, and this official will have my full support an regular access to me as we confront these challenges. Today, I want to focus on the important responsibilities this<br>office will fulfill: orchestrating and integrating all cybersecurity policies for the government; working closely with the Office of Management and Budget to ensure agency budgets reflect those priorities; and, **in the event of major cyber incident or attack, coordinating** | Capacidades cibernéticas para defenderse, asegurar, detectar amenazas en el ciberespacio | Innovación tecnológica en ciberseguridad<br><br>Respuestas |

| | | |
|---|---|---|
| **our response. To ensure that federal cyber policies enhance our security and our prosperity, my Cybersecurity Coordinator Will be a member of the National Security Staff** as well as the staff of my National Economic Council. To ensure that policies keep faith with our fundamental values, this office will also include an official with a portfolio specifically dedicated to safeguarding the privacy and civil liberties of the American people. | Mejoras en políticas y estrategias cibernéticas para tener una respuesta en caso de ataques | a incidentes cibernéticos |
| There's much work to be done, and the report we're releasing today outlines a range of actions that we will pursue in five key areas. First, working in partnership with the communities represented here today, **we will develop a new comprehensive strategy to secure America's information and communications networks.** To ensure a coordinated approach across government, my Cybersecurity Coordinator will work closely with my Chief Technology Officer, Aneesh Chopra, and my Chief Information Officer, Vivek Kundra to ensure accountability in federal agencies, cybersecurity will be designated as one of my key management priorities. Clear milestones and performances metrics will measure progress. and as we develop our strategy, we will be open and transparent, which is why you'll find today's report and a wealth of related information on our web site, www.whitehouse.gov. | Estrategia para asegurar la información y redes de comunicación | Reformas y revisiones en políticas sobre protección y seguridad de infraestructuras críticas de información |
| Second, we will work with all the key players including state and local governments and the private sector -- to ensure an organized and unified response to future cyber incidents. **Given the enormous damage that can be caused by even a single cyber attack, ad hoc responses will not do. Not is it sufficient to simply strengthen our defenses after incidents or attacks occur.** Just as we | Un solo ataque causa muchos daños, por eso se debe prevenir | Prevención y detención de ataques cibernéticos |

| | | |
|---|---|---|
| do for natural disasters, we have to have plans and resources in place beforehand sharing information, issuing warnings and ensuring a coordinated response. | | |
| Third, **we will strengthen the public/private partnerships that are critical to this endeavor**. The vast majority of our critical information infrastructure in the United States is owned and operated by the private sector. So let me be very clear: My administration will not dictate security standards for private companies. On the contrary, we will collaborate with industry to find technology solutions that ensure our security and promote prosperity. | Fortalecer alianzas entre el sector público y privado para proteger la infraestructura de información critica | Seguridad y protección de información |
| Fourth, we will continue to **invest in the cutting-edge research and development necessary for the innovation and discovery we need to meet the digital challenges of our time** and that's why my administration is making major investments in our information infrastructure: laying broadband lines to every corner of America; building a smart electric grid to deliver energy more efficiently; pursuing a next generation of air traffic control systems; and moving to electronic health records, with privacy protections, to reduce costs and save lives. and finally, **we will begin a national campaign to promote cybersecurity awareness and digital literacy** from our boardrooms to our classrooms, and to build a digital workforce for the 21st century and that's why we're making a new commitment to education in math and science, and historic investments in science and research and development. | Inversión en innovación tecnológica<br>Generar conciencia cibernética campañas nacional | Inversión en tecnología<br>Concientización sobre la importancia de la ciberseguridad |
| Because it's not enough for our children and students to master today's technologies social networking and emailing and texting and blogging -- we need them to pioneer the technologies | | |

| | | |
|---|---|---|
| that will allow us to work effectively through these new media and allow us to prosper in the future. So these are the things we will do let me also be clear about what we will not do. Our pursuit of cybersecurity will not include I repeat, will not include monitoring private sector networks or Internet traffic.<br><br>We will preserve and protect the personal privacy and civil liberties that we cherish as Americans. Indeed, I remain firmly committed to net neutrality so we can keep the Internet as it should be open and free. The task I have described will not be easy some 1.5 billion people around the world are already online, and more are logging on every day. **Groups and governments are sharpening their cyber capabilities. Protecting our prosperity and security in this globalized world is going to be a long, difficult struggle demanding patience and persistence over many years**. But we need to remember: We're only at the beginning. The epochs of history are long -- the Agricultural Revolution; the Industrial Revolution. **By comparison, our Information Age is still in its infancy. We're only at Web 2.0.**<br><br>Now our virtual world is going viral and we've only just begun to explore the next generation of technologies that will transform our lives in ways we can't even begin to imagine. So **a new world awaits a world of greater security and greater**<br>**potential prosperity** -- if we reach for it, if we lead. So long as I'm President of the United States, we will do just that and **the United States the nation that invented the Internet, that launched an information revolution, that transformed the world will do what we did in the 20th century and lead once more in the 21st.** | Aumentar capacidades cibernéticas es un nuevo reto<br><br>Necesidad de más seguridad<br><br>Mantener el liderazgo del siglo pasado | Innovación tecnológica en ciberseguridad<br><br>Innovación tecnológica en ciberseguridad<br><br>Prestigio internacional |

| | | |
|---|---|---|
| Thank you very much, everybody. | | |

Fuente: The White House, 2009
Elaborado por: Torres, P. (2020)

*Anexo 11. Análisis de contenido del segmento de las observaciones presidenciales por Barack Obama sobre la publicación de documentos clasificados por WikiLeaks*

| Titulo | Presidential Remarks on WikiLeaks Release of Classified Documents | |
|---|---|---|
| Intervención | Barack Obama | |
| Fecha de publicación | 27 de julio 2010 | |
| Emisor | The White House | |
| Texto transcripto | Códigos preliminares | Códigos finales |
| I know much has been written about this in recent days as a result of the substantial leak of documents from Afghanistan covering a period from 2004 to 2009.<br>While I am concerned about the disclosure of sensitive information from the battlefield that could potentially jeopardize individuals or operations, **the fact is these documents do not reveal any issues that have not been already informed our public debate on Afghanistan**; indeed, they point to the same challenges that led me to conduct an extensive review of our policy last fall.<br><br>So let me underscore what I have said many times: For seven years, we failed to implement a strategy adequate to the challenge in this region, the region from which the 9/11 attacks were waged and other attacks against the United States and our friends and allies have been planned.<br>That is why we have substantially increased our commitment there, insisted upon greater accountability from our partners in Afghanistan and Pakistan, developed a new strategy that can work, and put in place a team, including one of our finest generals, to execute that plan. | Las filtraciones no causan grandes daños | Afectaciones a las estrategias de EE. UU |

| | | |
|---|---|---|
| Now we have to see that strategy through.<br>And as I told the leaders, I hope the House will act today to join the Senate, which voted unanimously in favor of this funding, to ensure that our troops have the resources they need and that we are able to do what is necessary for our national security. | | |

Fuente: The White House, 2009
Elaborado por: Torres, P. (2020)

*Anexo. 12 Análisis de contenido del discurso del Presidente Obama sobre el crecimiento de las redes digitales ha aumentado la necesidad de invertir en seguridad en línea, así como los pasos que las personas pueden tomar para protegerse de las amenazas en el ciberespacio*

| Titulo | El presidente Obama explica cómo el crecimiento de las redes digitales ha aumentado la necesidad de invertir en seguridad en línea, así como los pasos que las personas pueden tomar para protegerse de las amenazas en línea. | |
|---|---|---|
| Intervención | Barack Obama | |
| Fecha de publicación | 14 de octubre del 2009 | |
| Emisor | The White House | |
| Texto transcripto | Códigos preliminares | Códigos finales |
| In this information age, the incredible technologies that we depend on every day present us with both great promise and great peril.<br><br>That's why I've designated October as **National Cyber Security Awareness Month, so we can seize the promise and confront the perils. Our digital networks are critical to our national security, our military superiority, and public safety, but that dependence also makes us vulnerable to Cyber attack from those who would do us harm**. The Internet and eCommerce are keys to our economic competitiveness.<br><br>But Cyber thieves have cost U.S. companies billions of dollars. As consumers we use the internet to pay our bills, to shop, to file our taxes. But | Concientización de seguridad cibernética para enfrentar los peligros y vulnerabilidades frente ataques cibernéticos | Concientización sobre la importancia de la ciberseguridad |

| | | |
|---|---|---|
| millions of Americans have been victimized, their privacy violated, their money and identity stolen, their lives turned upside down**. The lesson is clear: This Cyber threat is one of the most serious economic and national security challenges we face as a nation**. | Amenazas cibernéticas son un gran desafío | Amenazas cibernéticas |
| In this interconnected world, our vulnerability is shared, and so is our responsibility to protect ourselves. Government has the responsibility to lead. **That's why I've called for a new comprehensive approach to protecting America's digital infrastructure**. **My administration has recognized our networks as strategic national assets. It has made defending them a national security priority.** And to guide our efforts I created a new office here at the White House to be led by a Cyber security coordinator that I will soon appoint. The private sector has responsibilities as well. Most of America's critical information infrastructure is owned and operated by the private sector, by industry, hospitals, and academia. | Nuevo enfoque en proteger La infraestructura digital de EE. UU<br>Las redes de EE. UU como activos nacionales estratégicos, su defensa es una prioridad de seguridad nacional | Reformas y revisiones en políticas sobre protección y seguridad de infraestructuras críticas de información |
| So we need public **private partnerships and innovative Cyber Security solutions** that ensure both economic prosperity and personal privacy. Ultimately though, neither government nor the private sector alone can ensure our Cyber Security. Ultimately it comes down to each of us as individuals. It comes down to you. Whether at work, home or school, whether you're a parent or a child, there are simple steps you can take to stay safe online.<br><br>Keep your security software and systems up to date and beware of suspicious e-mails.<br>Always know who you're dealing with, whether it's a business or an individual. | Soluciones de ciberseguridad | Innovación tecnológica en ciberseguridad |

| | | |
|---|---|---|
| And never give out your personal or financial information until you verified that the recipient is legitimate. There's so many ways to be Cyber smart.<br>To learn more, visit OnGuardOnline.gov or DHS.Gov/Cyber.<br><br>**The technologies of our time bind us together like never before, but just as they empower others to disrupt and destroy**, we must harness them to learn, to create and to build.<br><br>That's our shared opportunity and our shared responsibility. Not only during National Cyber Security Awareness Month, but every time we go online. | Empoderamiento a diferentes tipos de actores para causar daños | Empoderamiento de actores no estatales en el ciberespacio |

Fuente: The White House, 2009
Elaborado por: Torres, P. (2020)

*Anexo 13. Análisis de contenido sobre la Declaración del Presidente sobre el Marco de Ciberseguridad*

| Titulo | Declaración del Presidente sobre el Marco de Ciberseguridad | |
|---|---|---|
| Intervención | Barack Obama | |
| Fecha de publicación | 12 de febrero del 2014 | |
| Emisor | The White House – Office of the Press Secretary | |
| Texto transcripto | Códigos preliminares | Códigos finales |
| Cyber threats pose one the gravest national security dangers that the United States faces. To better defend our nation against this systemic challenge, one year ago **I signed an Executive Order directing the Administration to take steps to improve information sharing with the private sector, raise the level of cybersecurity across our critical infrastructure, and enhance privacy and civil liberties**. | Mejoras en el intercambio de información para elevar la ciberseguridad de las infraestructuras críticas | Ciberseguridad para proteger información de intrusos externos |

| | | |
|---|---|---|
| Since then, the National Institute of Standards and Technology has worked with **the private sector to develop a Cybersecurity Framework that highlights best practices and globally recognized standards so that companies across our economy can better manage cyber risk to our critical infrastructure**. Today I was pleased to receive the Cybersecurity Framework, which reflects the good work of hundreds of companies, multiple federal agencies, and contributors from around the world. This voluntary Framework is a great example of how the private sector and government can, and should, work together to meet this shared challenge. | Mejorar la gestión del riesgo cibernético | Especialistas en ciberseguridad para evaluar riesgos y amenazas cibernéticas |
| While I believe today's Framework marks a turning point, it's clear that much more work needs to be done to **enhance our cybersecurity**. America's economic prosperity, national security, and our individual liberties **depend on our commitment to securing cyberspace and maintaining an open, interoperable, secure, and reliable Internet. Our critical infrastructure continues to be at risk from threats in cyberspace**, and our economy is harmed by the theft of our intellectual property. Although the threats are serious and they constantly evolve, I believe that if we address them effectively, we can ensure that the Internet remains an engine for | Asegurar el ciberespacio depende del compromiso de toda la nación | Protección de la nación en el ciberespacio |

| | | |
|---|---|---|
| economic growth and a platform for the free exchange of ideas.<br><br>I again urge Congress to move forward on cybersecurity legislation that both protects our nation and our privacy and civil liberties. Meanwhile, **my Administration will continue to take action, under existing authorities, to protect our nation from this threat**. | Seguir tomando medidas para proteger a la nación de amenazas cibernéticas | Mayor preparación en ciberseguridad |

Fuente: The White House, 2014
Elaborado por: Torres, P. (2020)

*Anexo. 14 Análisis de Contenido del segmento de la entrevista a Howard Schmidt en donde responde preguntas sobre el Mes nacional de concientización sobre ciberseguridad, la iniciativa "Stop.Think.Connect" para fomentar la seguridad en línea y formas de protegerse en línea.*

| Titulo | Howard Schmidt responde sus preguntas sobre el Mes nacional de concientización sobre ciberseguridad, la iniciativa "Stop.Think.Connect" para fomentar la seguridad en línea y formas de protegerse en línea. | |
|---|---|---|
| Intervención | Howard Schmidt coordinador de ciberseguridad | |
| Fecha de publicación | 20 de octubre de 2010. | |
| Emisor | The White House | |
| Texto transcripto | Códigos preliminares | Códigos finales |
| All of these things are run by technology today, and we're very fortunate to have that technology available to us. But **even with that, there are forces out there, bad guys and bad actors, as we call them, that look to do everything, to commit crimes like identity theft, credit card fraud, shutting down systems, for all kinds of reasons. And our job in the President's direction is to make sure that we minimize the likelihood any of these things will have a long-term effect or even for most cases how we can help people do that shared responsibility of protecting themselves. Cyber Security** | Reducir vulnerabilidades en el ciberespacio | Encontrar vulnerabilidades y fallas en las redes del gobierno |

| | | |
|---|---|---|
| **Awareness month, this is the seventh year we've been doing this.**<br><br>It's probably the biggest and baddest seventh anniversary celebration we've had for Cyber security awareness month yet. | | |
| **Some countries work hard to make sure that only approved information is available to their own citizens on the web. Does the Obama administration regard the wide open and freewheeling character of the Internet as a national security asset or liability?**<br><br>Howard Schmidt: Well, Dan, thanks for that question, because when we look at what we use the Internet for, as I mentioned in my comment a moment ago, everything from communications to entertainment, but the administration looks at it as a vehicle by which that we can communicate freely internationally.<br><br>So when we start looking at things about content and discussions of things that I think we all hold very dear to us from a democracy standpoint, we **believe that it is a national asset to be able to do that, which is consistent with the way our government has been built and the way we all live our online world. And the thing is that we need to work collaboratively internationally to make sure we protect those freedoms online, make sure that we're doing the things we need to do to give us the ability to do that, while protecting the technology at the same time.** | Seguridad como activo nacional | Reformas y revisiones en políticas sobre protección y seguridad de infraestructuras críticas de información |
| **What is the greatest single Cyber security issue or threat that you, Mr. Schmidt, use today?**<br><br>Howard Schmidt: You know, that's a really good question, Zach, because when we start looking about the things | Surgimiento de amenazas en el internet | Amenazas cibernéticas |

| | | |
|---|---|---|
| that people ask me all the time is what keeps you up at night, and I think the biggest thing is when we designed the Internet as we know it today, we built the applications, we built the routers, we built the Wi-FI network, we didn't fully realize, in many cases, that **bad things were going to happen like they have today.**<br><br>**So, we didn't pay a lot of attention to reducing the vulnerabilities And that's sort of the biggest thing today is, how do we wind up reducing the vulnerabilities to make sure we're better protected?**<br><br>And there's some ways to do that, and of course National Cyber Security Awareness month gives us a lot of those tools. | Reducir vulnerabilidades es el mayor reto del gobierno | Protección de la nación en el ciberespacio |
| **Is there a Cyber security emergency plan in place so that in case of an emergency, Cyber terrorists do not attack our critical technology infrastructure?**<br><br>Howard Schmidt: And thanks for that question, Harad, because when we start looking at the fact that if there continues to be people committing criminal acts out there and doing things to affect our infrastructure, one of the key things that the government needs to do is put together an instant response plan. **This is what we call the National Cyber Incident Response plan, or the NCIR.** Just a few weeks ago we had this international exercise called **Cyber Storm III** that brought in resources from, I think, more than 11 countries, more than 2,000 people worldwide, 31 private sector agencies, as well as the broad group of government agencies, to come and exercise this incident response plan, **which not only gives us the ability to identify what we've got going, but it's a great learning experience, because** | Planes e iniciativas de respuesta frente a incidentes cibernéticos para reducir los efectos y fomentar la recuperación rápida ante ataques | Políticas, estrategias, programas y leyes de ciberseguridad |

| | | |
|---|---|---|
| **as technology changes, as we become more dependent upon, say, peer-to-peer technologies, and the ability to communicate on a real time basis**, by bringing this instant response plan together, it doesn't make any difference what the person's motivation is, whether they come from anywhere in the world, that we have a plan in place that we bring all of government together, we bring all private sector together, **we bring all international partners together, to make sure that the impact is minimal, it's the shortest duration, and we have the ability to recover in the quickest time period possible.** | | |
| **What steps will the federal government take to facilitate the hiring of new Cyber security in privacy professionals?**<br><br>Howard Schmidt: You know, Greg, that's wonderful, because that's one of the things we've been talking about for a long time is, how do we **get more technology specialists, particularly in the area of Cyber security**, into the workforce across the government? Well, we have this **initiative called the National Initiative for Cyber Security Education, which in addition to Cyber Security Awareness month, we look at workforce development inside the private sector, the university courses that are available, the high school courses available, to really generate the next generation of technology specialists that focus on Cyber security**. | Especialistas en tecnología enfocado en el área de ciberseguridad | Especialistas en ciberseguridad para evaluar riesgos y amenazas cibernéticas |
| **Can transparency build better work spaces, or will it create toxic business areas?**<br>Howard Schmidt**: I think transparency will build a better work environment for us.And I think back to the President's commitment earlier this year about** | | |

| | | |
|---|---|---|
| **transparency. For example, on the Cyber security environment, there was a document created called the Comprehensive National Cyber Security Initiative, or the CNCI, that the President directed declassifying that document, talking about how we're going to do a better job about protecting the technology we deploy within the U.S. government** and the private sector. So, in this case, when we start looking at the benefits we get from any workflow environment from technology, openness is better. | Iniciativa para proteger la tecnología del gobierno EE. UU | Innovación tecnológica en ciberseguridad |

Fuente: The White House, 2014
Elaborado por: Torres, P. (2020)

*Anexo 15. Análisis de contenido del segmento del discurso del presidente Obama sobre los resultados de la revisión de la Administración de los programas de inteligencia y cómo, a la luz de las nuevas tecnologías, podemos usarlos de una manera que proteja de manera óptima nuestra seguridad nacional*

| | | |
|---|---|---|
| Titulo | El presidente Obama sobre los resultados de la revisión de la Administración de los programas de inteligencia y cómo, a la luz de las nuevas tecnologías, podemos usarlos de una manera que proteja de manera óptima nuestra seguridad nacional | |
| Intervención | Barack Obama | |
| Fecha de publicación | 17 de enero del 2014 | |
| Emisor | The White House | |
| Texto transcripto | Códigos preliminares | Códigos |
| Throughout American history, **intelligence has helped secure our country and our freedoms.** In the Civil War, Union balloon reconnaissance tracked the size of Confederate armies by counting the number of campfires. In World War II, code-breakers gave us insights into Japanese war plans, and when Patton marched across Europe, **intercepted communications helped save the lives of his troops**. After the war, the rise of the Iron Curtain and nuclear weapons only increased the need for sustained intelligence gathering. And so, in the early days of the Cold War, President Truman created the National Security Agency, or NSA**, to give us** | El rol de la información para las agencias de inteligencia del gobierno | Proteger la Seguridad Nacional |

| | | |
|---|---|---|
| **insights into the Soviet bloc, and provide our leaders with information they needed to confront aggression and avert catastrophe.** Throughout this evolution, we benefited from both our Constitution and our traditions of limited government**. U.S. intelligence agencies were anchored in a system of checks and balances -- with oversight from elected leaders, and protections for ordinary citizens.** Meanwhile, totalitarian states like East Germany offered a cautionary tale of what could happen when vast, unchecked surveillance turned citizens into informers, and persecuted people for what they said in the privacy of their own homes.<br><br>If the fall of the Soviet Union left America without a competing superpower, emerging threats from terrorist groups, and the proliferation of weapons of mass destruction placed new and in some ways more complicated demands on our intelligence agencies. **Globalization and the Internet made these threats more acute, as technology erased borders and empowered individuals to project great violence, as well as great good. Moreover, these new threats raised new legal and new policy questions.** For while few doubted the legitimacy of spying on hostile states, our framework of laws was not fully adapted to prevent terrorist attacks by individuals acting on their own, or acting in small, ideologically driven groups on behalf of a foreign power.<br><br>And it is a testimony to the hard work and dedication of the men and women of our **intelligence community that over the past decade we've made enormous strides in fulfilling this mission**. Today, new capabilities allow intelligence agencies to track | Amenazas graves por el surgimiento de actores no estatales | Empoderamiento de actores no estatales en el ciberespacio |

| | | |
|---|---|---|
| who a terrorist is in contact with, and follow the trail of his travel or his funding. **New laws allow information to be collected and shared more quickly and effectively between federal agencies, and state and local law enforcement. Relationships with foreign intelligence services have expanded, and our capacity to repel cyber-attacks have been strengthened. And taken together, these efforts have prevented multiple attacks and saved innocent lives -- not just here in the United States, but around the globe.** | Nuevas capacidades cibernéticas para repeler ataques cibernéticos | Innovación tecnológica en ciberseguridad |
| First, the same technological advances that allow U.S. intelligence agencies to pinpoint an al Qaeda cell in Yemen or an email between two terrorists in the Sahel also mean that many routine communications around the world are within our reach. **And at a time when more and more of our lives are digital, that prospect is disquieting for all of us**. | | |
| **Second, the combination of increased digital information and powerful supercomputers offers intelligence agencies the possibility of sifting through massive amounts of bulk data to identify patterns or pursue leads that may thwart impending threats. It's a powerful tool. But the government collection and storage of such bulk data also creates a potential for abuse.** | Identificar y frenar amenazas por el uso de infraestructura digital e información en el ciberespacio | Innovación tecnológica en ciberseguridad |
| Third, the legal safeguards that restrict surveillance against U.S. persons without a warrant do not apply to foreign persons overseas. This is not unique to America; few, if any, spy agencies around the world constrain their activities beyond their own borders. And **the whole point of intelligence is to obtain information that is not publicly available. But America's capabilities are unique,** | Poder de las nuevas tecnologías | Ciberpoder |

| | | |
|---|---|---|
| **and the power of new technologies means that there are fewer and fewer technical constraints on what we can do. That places a special obligation on us to ask tough questions about what we should do.** | | |
| And given the fact of an open investigation, I'm not going to dwell on Mr. Snowden's actions or his motivations**; I will say that our nation's defense depends in part on the fidelity of those entrusted with our nation's secrets. If any individual who objects to government policy can take it into their own hands to publicly disclose classified information, then we will not be able to keep our people safe, or conduct foreign policy**. Moreover, the sensational way in which these disclosures have come out has often shed more heat than light, while revealing methods to our adversaries that could impact our operations in ways that we may not fully understand for years to come. | La seguridad nacional depende de la protección de la información secreta de la nación | Seguridad y protección de la información |
| Regardless of how we got here, though, the task before us now is greater than simply repairing the damage done to our operations or preventing more disclosures from taking place in the future. Instead, **we have to make some important decisions about how to protect ourselves and sustain our leadership in the world, while upholding the civil liberties and privacy protections that our ideals and our Constitution require**. **We need to do so not only because it is right, but because the challenges posed by threats like terrorism and proliferation and cyber-attacks are not going away any time soon. They are going to continue to be a major problem. And for our intelligence community to be effective over the long haul, we must maintain the** | Aumentar protección y liderazgo en el mundo<br><br>Constantes ataques cibernéticos que aumentarán y serán el mayor problema | Prestigio Internacional<br>Liderazgo en el ciberespacio<br><br>Amenazas cibernéticas |

| | | |
|---|---|---|
| **trust of the American people, and people around the world.**<br><br>This effort will not be completed overnight, and given the pace of technological change, we shouldn't expect this to be the last time America has this debate. But **I want the American people to know that the work has begun. Over the last six months, I created an outside Review Group on Intelligence and Communications Technologies to make recommendations for reform. I consulted with the Privacy and Civil Liberties Oversight Board, created by Congress. I've listened to foreign partners, privacy advocates, and industry leaders. My administration has spent countless hours considering how to approach intelligence in this era of diffuse threats and technological revolution**. So before outlining specific changes that I've ordered, let me make a few broad observations that have emerged from this process.<br><br>First**, everyone who has looked at these problems, including skeptics of existing programs, recognizes that we have real enemies and threats, and that intelligence serves a vital role in confronting them. We cannot prevent terrorist attacks or cyber threats without some capability to penetrate digital communications -- whether it's to unravel a terrorist plot; to intercept malware that targets a stock exchange; to make sure air traffic control systems are not compromised; or to ensure that hackers do not empty your bank accounts. We are expected to protect the American people; that requires us to have capabilities in this field.**<br><br>Meanwhile, a number of countries, including some who have loudly criticized the NSA, privately | Acciones para mejorar las tecnologías de inteligencia, información y comunicaciones<br><br>Enemigos reales en el ciberespacio | Políticas, estrategias, programas y leyes de ciberseguridad<br><br>Hackers |

| | | |
|---|---|---|
| **acknowledge that America has special responsibilities as the world's only superpower; that our intelligence capabilities are critical to meeting these responsibilities, and that they themselves have relied on the information we obtain to protect their own people.** | EE.UU única superpotencia del mundo con la función de proteger el ciberespacio con sus capacidades de inteligencia | Ciberpoder |
| Second, just as ardent civil libertarians recognize the need for robust intelligence capabilities, **those with responsibilities for our national security readily acknowledge the potential for abuse as intelligence capabilities advance and more and more private information is digitized**. | Necesidad de implementar más capacidades de inteligencia | Mayor preparación en ciberseguridad |
| I've also made it clear that the United States does not collect intelligence to suppress criticism or dissent, nor do we collect intelligence to disadvantage people on the basis of their ethnicity, or race, or gender, or sexual orientation, or religious beliefs. We do not collect intelligence to provide a competitive advantage to U.S. companies or U.S. commercial sectors.<br><br>And in terms of our bulk collection of signals intelligence, **U.S. intelligence agencies will only use such data to meet specific security requirements: counterintelligence, counterterrorism, counter-proliferation, cybersecurity, force protection for our troops and our allies, and combating transnational crime, including sanctions evasion.** | Recopilar información para cumplir con operaciones de seguridad | Proteger la seguridad nacional |
| Finally, to make sure that we follow through on all these reforms, I am making some important changes to how our government is organized. **The State Department will designate a senior officer to coordinate our diplomacy on issues related to technology and signals intelligence. We will appoint a senior official at** | Iniciativas en temas de inteligencia y tecnología para combatir crimen y terrorismo | Políticas, estrategias, programas y |

| | | |
|---|---|---|
| **the White House to implement the new privacy safeguards that I have announced today. I will devote the resources to centralize and improve the process we use to handle foreign requests for legal assistance, keeping our high standards for privacy while helping foreign partners fight crime and terrorism.** | | leyes de ciberseguridad |
| Whether it's the ability of individuals to communicate ideas; to access information that would have once filled every great library in every country in the world; or to forge bonds with people on other sides of the globe**, technology is remaking what is possible for individuals, and for institutions, and for the international order. So while the reforms that I have announced will point us in a new direction, I am mindful that more work will be needed in the future.** | Incrementar tecnología | Innovación tecnológica en ciberseguridad |
| One thing I'm certain of: This debate will make us stronger. And **I also know that in this time of change, the United States of America will have to lead.** It may seem sometimes that America is being held to a different standard. And I'll admit the readiness of some to assume the worst motives by our government can be frustrating | Liderazgo de EE.UU | Liderazgo en el ciberespacio |
| **As the nation that developed the Internet, the world expects us to ensure that the digital revolution works as a tool for individual empowerment, not government control. Having faced down the dangers of totalitarianism and fascism and communism, the world expects us to stand up for the principle that every person has the right to think and write and form relationships freely -- because individual freedom is the wellspring of human progress.** | Responsabilidad de garantizar la revolución digital en el mundo | Ciberpoder |

| | | |
|---|---|---|
| | | |

Fuente: The White House, 2014
Elaborado por: Torres, P. (2020)

*Anexo 16. Análisis de Contenido del discurso del Presidente Obama sobre seguridad*

| Titulo | El presidente habla sobre seguridad | |
|---|---|---|
| Intervención | Barack Obama | |
| Fecha de publicación | 13 de enero del 2015 | |
| Emisor | National Cybersecurity and Communications Integration Center | |
| Texto transcripto | Códigos preliminares | Códigos finales |
| Yesterday, I announced new proposals to better **protect Americans from identity theft and to ensure our privacy**, including making sure that our kids are safe from digital marketing and intrusions on their privacy based on what they're doing at school. Tomorrow in Iowa, I'll talk about how we can give more families and communities faster, cheaper access to the broadband that allows them to successfully compete in this global economy. And on Thursday, the Vice President will be in Norfolk to highlight the need to continue to invest in the education and skills for our cybersecurity professionals. But today I am here at DHS to highlight how we can work with the private sector to better **protect American companies against cyber threats.** | Iniciativas para mejorar la privacidad de información y aumentar la protección frente a amenazas cibernéticas | Políticas, estrategias, programas y leyes de ciberseguridad |
| Shortly after I took office, I declared that **cyber threats pose an enormous challenge for our country. It's one of the most serious economic and national security challenges we face as a nation. Foreign governments, criminals and hackers probe America's computer networks every single day.** We saw that again with the attack at Sony, which actually destroyed data and computer hardware that is going to be very costly for that company to clean up. Just yesterday, we saw the hack of a military Twitter | Amenazas cibernéticas desafío más grande para la seguridad nacional<br><br>Ataques diarios a las redes del gobierno por diferentes actores | Globalización<br><br>Hackers criminales |

| | | |
|---|---|---|
| account and You Tube channel. No military operations were impacted. So far, it appears that no classified information was released. But the investigation is ongoing, and it's a reminder that **cyber threats are an urgent and growing danger.** | Peligros en el ciberespacio tienen un creciente potencial de daño | Amenazas cibernéticas |
| And that's why I've said that **protecting our digital infrastructure is a national security priority and a national economic priority**. Over the **past six years, we've pursued a comprehensive strategy, boosting our defenses in government, sharing more information with the private sector to help them defend themselves, working with industry through what we call the Cybersecurity Framework not just to respond to threats and recover from attacks but to prevent and disrupt them in the first place.** | En los últimos 6 años las estrategias se han basado en aumentar defensas, responder amenazas, irrumpir, prevenir y recuperarse de ataques | Reformas y revisiones en políticas sobre protección y seguridad de infraestructuras críticas de información |
| And that's where these good folks come in. We are currently at the National Cybersecurity Communications Integration Center -- also known as NCCIC. I just got a tour and a briefing. I want to thank everybody here, not just from DHS but from across government and the private sector, because, again, this is a shared responsibility.<br>This center is one of the critical lines of America's cyber defenses. These men and women work around the clock, 24/7, monitoring threats, issuing warnings, sharing information with the private sector, and keeping Americans safe. So, as a nation, we owe them thanks, and as a nation, **we are making progress. We're more prepared to defend against cyber attacks. But every day, our adversaries are getting more sophisticated and more determined, and more plentiful. So every day, we've got to keep upping our game at the same time. We've got to stay ahead of those who are trying to do us harm.** | Crecimiento de dificultades y enemigos en el ciberespacio.<br><br>Constante aumento de capacidades cibernéticas | Globalización<br><br>Innovación tecnológica en ciberseguridad |

| | | |
|---|---|---|
| The problem is that government and the private sector are still not always working as closely together as we should. **Sometimes it's still too hard for government to share threat information with companies. Sometimes it's still too hard for companies to share information about cyber threats with the government.** There are legal issues involved and liability issues. Sometimes, companies are reluctant to reveal their vulnerabilities or admit publicly that they have been hacked. At the same time, the American people have a legitimate interest in making sure that government is not potentially abusing information that it's received from the private sector.<br>So all of us -- government and industry -- are going to have to keep doing better. The new legislation and proposals I put forward yesterday will help, especially for a strong, single national standard for notifying Americans when their information has been breached. Today, I want to announce some additional steps.<br>First, **we're proposing new cybersecurity legislation to promote the greater information sharing** we need between government and the private sector. This builds and improves upon legislation that we've put forward in the past. It reflects years of extensive discussions with industry. It includes liability protections for companies that share information on cyber threats. It includes essential safeguards to ensure that government protects privacy and civil liberties even as we're doing our job of **safeguarding America's critical information networks.**<br><br>I raised this issue again and the need for this legislation with congressional leaders this morning, including Speaker | Compartir información sobre amenazas cibernéticas entre actores estatales y empresas para aumentar seguridad y reducir amenazas<br><br>Nueva legislación de seguridad cibernética – mejoras en el compartimiento de información | Revisión de las prácticas de seguridad<br><br>Reformas y revisiones en políticas sobre protección y seguridad de infraestructuras críticas de información |

| | | |
|---|---|---|
| Boehner and Leader McConnell, and we all agree that this is a threat that has to be addressed, and I am confident that we should be able to craft bipartisan legislation soon to put these systems in place. **We're going to keep on working with Congress to get this done. And in the meantime, we're going to do everything we can with our existing authorities to make sure industry gets the information it needs to better defend itself.** | Continuar con los esfuerzos de protección de información para mejorar las acciones de defensa | Seguridad y protección de información |
| Second, **we're proposing to update the authorities that law enforcement uses to go after cyber criminals. We want to be able to better prosecute those who are involved in cyber attacks**, those who are involved in the sale of cyber weapons like botnets and spyware. **We want to ensure that we're able to prosecute insiders who steal corporate secrets or individuals' private information.** And we want to expand the authority of courts to shut down botnets and other malware. The bottom line, **we want cyber criminals to feel the full force of American justice, because they are doing as much damage**, if not more, these days as folks who are involved in more conventional crime. | Perseguir cyber criminales que roban información secreta y ejecutan ataques cibernéticos | Hackers |
| Because they're hard and they're complicated issues. But if we keep on working on them together, and focus on concrete and pragmatic steps that we can take to **boost our cybersecurity and our privacy, I'm confident that both our privacy will be more secure and our information, our networks, public health, public safety will be more secure. We're going to keep on at this as a government, but we're also going to be working with the private sector to detect, prevent, defend, deter against attacks, and to recover quickly from any disruptions or damage**. And as long as I'm President, protecting **America's digital** | Continuar incrementando seguridad cibernética es un tema de prioridad nacional | Fortalecimiento en todo aspecto de la Ciberseguridad |

| | | |
|---|---|---|
| **infrastructure is going to remain a top national security priority.**<br><br>In closing, I want to say one of the areas I'll be working with Congress is to ensure that we don't let any disagreements keep us from fulfilling our most basic responsibilities. Last week's attack in Paris was a painful reminder that we have no greater duty than the security of the American people. And our national security should never be subject to partisan political games. **Congress needs to fully fund our Department of Homeland Security**, without delay, so that the dedicated public servants working here can operate with the certainty and confidence they need to keep the American people safe. And that's true across the board in the Department of Homeland Security.<br>So, again, I want to thank Jeh and Deputy Secretary Mayorkas, and everybody here at NCCIC and DHS for the great job you are doing. You are helping to keep the nation safe and secure.<br>And with that, we're going to get out of here so you can get back to work. Who knows what's been happening while you've been paying attention to me? (Laughter.) All right? Thank you very much, everybody. (Applause.) | Mayor financiamiento al Departamento de Seguridad Nacional | Inversión en tecnología |

Fuente: National Cybersecurity and Communications Integration Center, 2015
Elaborado por: Torres, P. (2020)

*Anexo. 17 Análisis de contenido del discurso de la Asistente del Presidente de Seguridad Nacional y Contraterrorismo Lisa O. Mónaco sobre el fortalecimiento de las ciberdefensas de EE. UU*

| | | |
|---|---|---|
| Titulo | Fortalecimiento de las ciberdefensas de EE. UU | |
| Intervención | Asistente del Presidente de Seguridad Nacional y Contraterrorismo Lisa O. Mónaco | |
| Fecha de publicación | 10 de febrero del 2015 | |
| Emisor | The Wilson Center Washington D.C | |
| Texto transcripto | Códigos preliminares | Códigos |

| | | |
|---|---|---|
| As President Obama's Homeland Security and Counterterrorism Advisor, I brief him every morning on the most significant, destructive, and horrific threats facing the American people. I am oftentimes, as the President reminds me, the "bearer of bad news." Since I began this job two years ago, I can tell you that an increasing share of the bad news **I deliver is unfortunately on cyber threats**. In just the last nine months, we've seen a growing list of high profile targets – Home Depot, JP Morgan Chase, Target, Sony Pictures, CENTCOM, and the U.S. Postal Service, to name a few.<br><br>We are at a transformational moment in the evolution of the cyber threat. The actions we take today – and those we fail to take – will determine **whether cyberspace remains a great national asset or increasingly becomes a strategic liability. An economic and national security strength, or a source of vulnerability.** | Amenazas más destructivas y terribles<br><br>Ciberespacio como una responsabilidad estratégica, o una fuente de vulnerabilidad | Amenazas cibernéticas<br><br>Globalización |
| So today, I want to talk about the threat we face and the Administration's approach to countering it, drawing on counterterrorism lessons learned from the last decade of war.<br><br>Let me start with the facts. **According to a recent U.S. Government assessment, cyber threats to our national and economic security are increasing in their frequency, scale, sophistication, and severity of impact. The range of cyber threat actors, methods of attack, targeted systems, and victims are expanding at an unprecedented clip**.<br><br>The pace of **cyber intrusions has also ticked up substantially**—annual reports of data breaches have | Ataques y actores cibernéticos incrementando y mejorando constantemente<br><br>Incremento de intrusiones cibernéticas en violación de datos e información | Empoderamiento de actores no estatales en el ciberespacio<br><br>Amenazas cibernéticas |

| | | |
|---|---|---|
| increased roughly five-fold since 2009. And the seriousness of those breaches is also rising, causing significant economic damage.<br><br>No one, it seems, is immune – from healthcare companies and universities to the tech industry, critical infrastructure, and entertainment sector. Just last week, Anthem, one of the nation's largest health insurance providers, announced that hackers had breached a database containing the personal information of 80 million customers and employees. **Inside the U.S. government, we know that state and non-state actors, terrorists, hackers, and criminals are probing our networks every day – seeking to steal, spy, manipulate, and destroy data.** | Actores empoderados en el ciberespacio para causar disrupción | Hackers |
| **At the state level, threats come from nations with highly sophisticated cyber programs, including China and Russia, and nations with less technical capacity but greater disruptive intent, like Iran and North Korea. Several nations regularly conduct cyber economic espionage for the commercial gain of their companies**. And politically motivated attacks are a growing reality, as we saw with North Korea's attack on South Korean banks and media outlets last year.<br><br>As for non-state actors, threats are increasingly originating from profit-motivated criminals—**so-called hackers** for hire—those who steal your information and sell it to the highest bidder online. **Transnational criminals use cyber as a vector for profit. There are the ideologically motivated hackers or terrorists**. **You have groups like Anonymous that thrive on creating disruptions on company's websites and leaking personal information** | Amenazas de otros estados con programas cibernéticos sofisticados para operaciones de espionaje cibernético<br><br>Actores no estatales para obtener ganancias, filtrar información en línea y tienen motivaciones ideológicas | Amenazas cibernéticas<br><br>Hackers |

| | | |
|---|---|---|
| **online.** You have groups like the so-called Syrian Electronic Army, which conducts cyber attacks in support of the brutal regime in Syria. And then there is ISIL, which has harnessed social media for a propaganda machine that's radicalizing and recruiting young people to their hateful message around the world. | | |
| Most concerning, perhaps, is **the increasingly destructive and malicious nature of cyber attacks**, as we saw with Sony Pictures Entertainment last fall. This attack stole large amounts of data and rendered inoperable thousands of Sony's computers and servers. It was a game changer because it wasn't about profit—it was about a dictator trying to impose censorship and prevent the exercise of free expression. At bottom, it was about coercion, which the United States believes is unacceptable, and which is why we took the extraordinary step of publicly identifying North Korea as responsible for the attack and responded swiftly, imposing additional sanctions on Kim Jong-Un's regime.I**n short, the threat is becoming more diverse, more sophisticated, and more dangerous.**<br><br>And I worry that malicious attacks like the one on Sony Pictures will increasingly become the norm unless we adapt quickly and take a comprehensive approach, just as we have in other contexts. Which brings me to the counterterrorism model. **Now, to be sure, there are many differences that make it difficult to apply lessons learned from the counterterrorism experience to cyber**. For one, the **private sector plays a more central role in spotting and responding to cyber incidents than they do in the** | Naturaleza destructiva y maliciosas de las amenazas cibernéticas<br><br>Acciones privadas y gubernamentales frente a los ataques en el ciberespacio | Afectaciones a la seguridad nacional<br><br>Prevención y detención de ataques cibernéticos |

| | | |
|---|---|---|
| **counterterrorism realm, where the government largely takes the lead.**<br><br>Having observed our Nation's response to terrorism post 9/11 from three different perches in the U.S. government—at the FBI, as Assistant Attorney General for National Security at the Department of Justice, and now at the White House—I can tell you there are structural, organizational, and cultural shifts that were made in our government in the counterterrorism realm that also apply to cyber. **We need to develop the same muscle memory in the government response to cyber threats as we have for terrorist incidents**.<br><br>Structurally, since 9/11 our government has done the hard work of breaking down walls in our counterterrorism agencies and bringing people together to share information so that we get the best possible assessment of the threat. **Whenever possible, we're bringing partners together to share information and extend our operational reach.** This model has made our counterterrorism mission against an evolving enemy more effective and sustainable. | Desarrollo de capacidades de respuesta frente a ataques y amenazas cibernéticas | Innovación tecnológica en ciberseguridad |
| Like counterterrorism, meeting **cyber threats requires a whole-of-government approach that uses all the appropriate tools available to us—including our global diplomacy, our economic clout, our intelligence resources, our law enforcement expertise, our competitive technological edge, and, when necessary, our military capability.** Those who would harm us should know that they can be found and will be held to account.<br><br>**In the cyber context, we need to share threat information more** | Usar todas las herramientas de poder del gobierno frente a las ciberamenazas | Ciberpoder |

| | | |
|---|---|---|
| **broadly and coordinate our actions** so that we're all working to achieve the same goal—and we have to do so consistent with our fundamental values and in a manner that includes appropriate protections for privacy and civil liberties**. We need to sync up our intelligence with our operations and respond quickly to threats against our citizens, our companies, and our Nation.** | Generar respuestas efectivas y de inteligencia frente a las amenazas | Innovación tecnológica en ciberseguridad |
| Make no mistake. Over the last few years, we have developed new and better ways to collaborate across all levels of government and with our partners in the private sector—including at the operational hubs in our government charged with **monitoring threats, issuing warnings, sharing information, and protecting America's critical infrastructure.** | Protección de la infraestructura crítica | Reformas y revisiones en políticas sobre protección y seguridad de infraestructuras críticas de información |
| At the White House, we've taken steps to improve our policy response. Last summer, **following a rising number of breaches and intrusions to public and private networks, we created the Cyber Response Group, or CRG**—modeled on the highly effective and long-standing Counterterrorism Security Group. **The CRG convenes the interagency and pools knowledge about ongoing threats and attacks and coordinates all elements of our government's response at the highest levels.** | Creación de grupos de respuesta cibernética a amenazas y ataques | Especialistas en ciberseguridad para evaluar riesgos y amenazas cibernéticas |
| Despite this progress, it has become clear that **we can do more as a government to quickly consolidate, analyze, and provide assessments on fast-moving threats or attacks.** As President Obama said during the State of the Union last month, **we will make "sure our government integrates intelligence** | Más esfuerzos para combatir las amenazas cibernéticas, así como se lucha contra el terrorismo | Prevención y detención de ataques cibernéticos |

| | | |
|---|---|---|
| **to combat cyber threats, just as we have done to combat terrorism."**<br><br>So today, I'm pleased to announce that we will establish a **new Cyber Threat Intelligence Integration Center, or CTIIC**, under the auspices of the Director of National Intelligence. **Currently, no single government entity is responsible for producing coordinated cyber threat assessments, ensuring that information is shared rapidly among existing Cyber Centers and other elements within the government, and supporting the work of operators and policy makers with timely intelligence about the latest cyber threats and threat actors. The CTIIC is intended to fill these gaps**.<br><br>In this vein, CTIIC will serve a similar function for cyber as the National Counterterrorism Center does for terrorism—**integrating intelligence about cyber threats; providing all-source analysis to policymakers and operators; and supporting the work of the existing Federal government Cyber Centers, network defenders, and local law enforcement communities. The CTIIC will not collect intelligence—it will analyze and integrate information already collected under existing authorities.**<br><br>Nor will it perform functions already assigned to other Centers. It is intended to enable them to do their jobs more effectively, and as a result, **make the Federal government more effective as a whole in responding to cyber threats**. CTIIC will draw on the existing Cyber Centers to better integrate their relevant expertise and information to improve our collective response to threats. | Nuevo centro de inteligencia especializado en ciberamenazas apoyando al trabajo de los Centros Cibernéticos existentes del gobierno federal, analizará e integrará la información ya recopilada<br><br>Mejorar la respuesta y la efectividad de las acciones del gobierno<br><br>Ciber es un área vital para la protección de la Seguridad Nacional en el presente y futuro | Instituciones de Ciberseguridad<br><br>Respuestas a incidentes cibernéticos<br><br>Proteger la seguridad nacional |

| | | |
|---|---|---|
| Of course, responding to today's threat is only part of the task. **The real challenge is getting ahead of where the threat is trending. That's why the President's National Security Strategy identifies cyber as a critical focus area to ensure we both meet the challenges of today and prepare for the threats we will face tomorrow.** The President's new budget backs up this commitment with **$14 billion to protect our critical infrastructure, government networks, and other systems.** And later this week, at Stanford University, President Obama and I and several Cabinet members will join hundreds of experts, academics, and private sector representatives for a first-of-its-kind summit to discuss how we can improve trust, enhance cooperation, and strengthen America's online consumer protections and cyber defenses. | Incremento de presupuesto para proteger los sistemas, redes e infraestructura crítica | Inversión en tecnología |
| But to truly safeguard Americans online and enhance the security of what has become a vast cyber ecosystem**, we are going to have to work in lock-step with the private sector**. The private sector cannot and should not rely on the government to solve all of its cybersecurity problems. **At the same time, I want to emphasize that the government won't leave the private sector to fend for itself. Partnership is a precondition of success—there's no other way to tackle such a complicated problem.** It requires daily collaboration to identify and analyze threats, address vulnerabilities, and then work together to respond jointly.<br><br>To the private sector, we've made it clear that we will work together. We're not going to bottle up our intelligence—if we have information about a significant threat | Asociaciones en conjunto para fomentar la seguridad del gobierno y de la población norteamericana | Cooperación en ciberseguridad |

| | | |
|---|---|---|
| to a business, we're going to do our utmost to share it. In fact, within 24 hours of learning about the Sony Pictures Entertainment attack, the U.S. government pushed out information and malware signatures to the private sector to update their cyber defenses. We want this flow of information to go both ways. **The private sector has vital information we don't always see unless they share it with us, and the government has a unique capacity to integrate information about threats, including non-cyber sources, to create the best possible picture to secure all of our networks.**<br><br>When companies share information with us about a major cyber intrusion or a potentially debilitating denial of service attack, they can expect us to respond quickly. We will provide as much information as we can about the threat to assist companies in protecting their networks and critical information. **We will coordinate a quick and unified response from government experts, including at DHS and the FBI. We will look to determine who the actor is and hold them to account. And, as we respond to attacks, we will bring to bear all of the tools available to us and draw on the full range of government resources to disrupt threats.** | Protección de información<br><br>Identificar actores que causan los ataques | Seguridad y protección de información<br><br>Hackers |
| I want to commend companies that have shown strong leadership by coming forward as soon as they identify breaches and seeking assistance so we can work together and address threats more rapidly—which is good for the company, good for the consumer, and good for the government. **Across the board, we're tearing down silos, increasing communication, and developing the flexibility and agility to respond to** | Aumentando constantemente capacidades cibernéticas | Innovación tecnológica en ciberseguridad |

| | | |
|---|---|---|
| **cyber threats of the 21st century, just as we have done in the counterterrorism world**. | | |
| Moving forward, as our lives become more **and more dependent on the Internet, and the amount of territory we have to defend keeps expandi**ng, our strategy will focus on four key elements. | Internet | Globalización |
| First, we need to improve our **defenses—employing better basic preventative cybersecurity, like the steps outlined in the Cybersecurity Framework announced last year, would enable every organization to manage cyber risk more effectively**. But even just employing basic cyber hygiene could stop a large percentage of the intrusions we face, so we've got to start by getting the basics rights. | Mejorar defensas al emplear mejor la seguridad cibernética | Prevención y detención de ataques cibernéticos |
| Second, we need **to improve our ability to disrupt, respond to, and recover from cyber threats. That means using the full strength of the United States government—not just our cyber tools—to raise the costs for bad actors and deter malicious actions.** | Mejoras en las acciones y esfuerzos de todo el gobierno para irrumpir, responder y recuperarse frente a amenazas cibernéticas de actores maliciosos | Fortalecimiento en todo aspecto de la Ciberseguridad |
| Third, we need to **enhance international cooperation, including between our law enforcement agencies, so that when criminals anywhere in the world target innocent users online, we can hold them accountable**—just as we do when people commit crimes in the physical world. | Impulsar Cooperación internacional para crear más leyes para el control y orden en el ciberespacio | Liderazgo en el ciberespacio |
| And fourth, we need to **make cyberspace intrinsically more secure—replacing passwords with more secure technologies, building more resilient networks, and enhancing consumer protections online, to start with**. | Hacer al ciberespacio un lugar seguro | Cooperación en ciberseguridad<br><br>Protección de la nación en el ciberespacio |

| | | |
|---|---|---|
| President Obama will **continue to do everything within his authority to harden our cyber defenses, but executive actions alone will not be enough. We need durable, long-term solutions, codified in law that bolster the Nation's cyber defenses.** This is not, and should not, be a partisan issue. The future security of the United States depends on a strong, bipartisan consensus that responds to a growing national security concern. Everyone shares responsibility here, including the Congress. | Mayor seguridad en la nación | Fortalecimiento en todo aspecto de la Ciberseguridad |
| In December, **Congress passed important bills to modernize how the government protects its systems and to clarify the government's authorities to carry out its cyber missions**. Today, we need the Congress to build on that **progress by passing the package of cybersecurity measures that President Obama announced last month that encourage greater information sharing**, set a national standard for companies to report data breaches, and provide law enforcement with updated tools to combat cybercrime. And we look to Congress to pass a budget with critical funding for cybersecurity, including for DHS. The Administration is ready to work with Congress to pass these measures as quickly as possible. | Proyectos de ley para modernizar la protección de sistemas redes e infraestructura | Reformas y revisiones en políticas sobre protección y seguridad de infraestructuras críticas de información |
| **Cybersecurity is and will remain a defining challenge of the 21st century**. With more than three billion internet users around the world and as many as ten billion internet-connected devices, there's no putting this genie back in the bottle. We have to get this right. **Our prosperity and security depend upon the Internet being secure against threats; reliable in our ability to access information; open to all who seek to** | Ciberseguridad el nuevo desafío<br><br>Prosperidad y seguridad dependen del ciberespacio | Políticas, estrategias, programas y leyes de ciberseguridad<br><br>Proteger la seguridad nacional |

| | | |
|---|---|---|
| **harness the opportunities of the Internet age; and interoperable to ensure the free flow of information across networks and nation**s.<br>But we are at a crossroads, and the clock is ticking. The choices we make today will define the threat environment we face tomorrow.<br><br>All of us have a responsibility to act—to take preventative measures to **defend our systems; to build greater resilience into our networks to bounce back from attacks; to break down silos and improve information sharing and the integration and analysis of threats; to pass cybersecurity legislation; and to ensure we take a comprehensive, whole-of-government approach to respond to cyber attacks, just as we do in other contexts.**<br><br>These are hard and complicated issues. But I'm confident that working together—government, industry, advocacy groups, the public, and Congress—our networks will be safer, our privacy protected, and our future more secure. I look forward to tackling these threats with all of you. Thanks very much. | Mayores oportunidades en la era del internet<br><br>Mayor resistencia en las redes, legislación sobre seguridad cibernética | Ataques cibernéticos y acciones disruptivas<br><br>Empoderamiento de actores no estatales en el ciberespacio<br><br>Respuestas a incidentes cibernéticos<br><br>Políticas, estrategias, leyes y programas de ciberseguridad |

Fuente: The Wilson Center Washington D.C, 2015
Elaborado por: Torres, P. (2020)