UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE CIENCIAS POLÍTICAS Y SOCIALES

LA POLÍTICA DE SEGURIDAD CIBERNÉTICA ESTADOUNIDENSE COMO PRIORIDAD NACIONAL E INTERNACIONAL DE 2001 A 2013: EL CASO DE LOS *CABLEGATES* DE WIKILEAKS

T E S I S

PARA OBTENER EL TÍTULO DE:

LICENCIADA EN RELACIONES INTERNACIONALES

P R E S E N T A:

XIMENA DOMÍNGUEZ CAMPUZANO

ASESOR

MTRO. JESÚS GUTIÉRREZ CASTRO

CIUDAD UNIVERSITARIA, MÉXICO D.F., OCTUBRE 2014

Agradecimientos

A mi mamá la persona que me ha enseñado a seguir adelante a pesar de los obstáculos, mi ejemplo de vida, mi confidente, mi gran maestra, por darme siempre tu opinión aún sin solicitarla, por tu infinita paciencia y gran cariño. A ti que me apoyaste y alentaste a seguir adelante cuando sentí que me rendía.

A mi papá que me ha enseñado a luchar incansablemente por mis sueños, que nunca me ha dejado caer, mi gran amigo, mi héroe, mi consejero, por tu cariño y amor incondicional. Este triunfo lo comporto con ustedes Irma y Guillermo, infinitas gracias porque ayudarme a ser lo que soy el día de hoy.

A mi abuelitos y familia por su apoyo y ánimos para lograr mis objetivos.

A mis queridas amigas, compañeras de vida que han estado a mi lado en todo momento, por los desvelos, esfuerzos, aventuras y desventuras que se han vuelto parte de mi historia. La vida nos tiene preparadas muchas sorpresas más nunca se rindan.

A mi querida Universidad Nacional Autónoma de México por inculcarme el amor a la lectura, al conocimiento, por permitirme cumplir mi sueño de la infancia, tener un corazón Azul y Oro.

A mi asesor y sinodales por tomarse el tiempo de leerme, por sus consejos y apoyo a lo largo de la realización de esta trabajo.

ÍNDICE

Índice de Tablas

Anexo

Introducción

Desde los atentados terroristas del 11 de septiembre de 2001 en Nueva York se dio un cambio de paradigma en las relaciones internacionales norteamericanas. A nivel discursivo la lucha contra el terrorismo fue vista como una amenaza para el mundo entero y bajo este argumento el gobierno de los Estados Unidos promovió la cooperación mundial para evitar que el terrorismo continuara afectando a las naciones. Es decir, el gobierno norteamericano estableció nuevas políticas y estrategias internacionales para enfrentar sus nuevos retos internos.

Este cambio de paradigma se vio reflejado en diferentes niveles: por ejemplo se endurecieron las fronteras norteamericanas, se incrementaron las alianzas estratégicas con otros países y el gobierno norteamericano endureció sus políticas de seguridad hacia el mundo entero, incrementando las medidas de vigilancia y monitoreo con la finalidad de mantener su seguridad nacional y la estabilidad mundial. Asimismo, se activó una alerta frente a los países de Medio Oriente, al considerar a esta zona como una amenaza latente para la seguridad mundial, porque era vista como una región que acogía terroristas y cuyo principal objetivo era desestabilizar a los gobiernos existentes.

Adicionalmente, el gobierno norteamericano analizó los riesgos del uso de las tecnologías de la información y definió como áreas estratégicas las políticas de seguridad informática y el resguardo del espacio cibernético. Se argumentó que el ciberespacio podría ser un lugar de confrontación y guerra, situación que anteriormente no se había manifestado.

Frente a estos nuevos retos, desarrolló nuevos sistemas de inteligencia como el sistema de Internet del ejército norteamericano, *Secret Internet Protocol Router Network* (SIPRNET) y estableció nuevas políticas de seguridad orientadas a evitar la fuga de información clasificada. Sin embargo, como observaremos a lo largo de esta tesis, en donde analizaremos el caso Wikileaks de 2001 a 20013, los esfuerzos norteamericanos fracasaron.

El objetivo general de esta investigación será analizar la evolución de las políticas de seguridad cibernética instrumentadas por el gobierno de los Estados Unidos desde 2001 hasta 2013, para entender cuáles fueron las fallas que hicieron posible la filtración de información por parte de los Cablegates y posteriormente analizar cuáles fueron las consecuencias internas y externas para este país.

Consideramos relevante analizar las causas que dificultaron el resguardo de la información dentro del ciberespacio, ya que era una prioridad del gobierno norteamericano. Destacaremos el rápido avance en la tecnología; el enorme volumen de información que este gobierno; la falta de capacitación del personal a cargo de la información reservada y el proceso de centralización de la información clasificada, lo cual permitió que estuviera al alcance de un gran número de empleados “de confianza”, debilitando los mecanismos de seguridad.

El caso Wikileaks que desarrolla a lo largo de la investigación es de naturaleza trascendente porque evidenció las debilidades y flaqueza del gobierno de los Estados Unidos y porque rompió con el mito de que el gobierno norteamericano era una potencia de inteligencia y de información con los más altos parámetros de seguridad en materia de información.

Por otra parte, el fenómeno de los *Cablagates* de Wikileaks, que implicó la filtración de 251,287 documentos del Departamento de Estado de los Estados Unidos sobre detalles ocultos, planes secretos y opiniones personales de los embajadores sobre algunos de los personajes más importantes de la esfera internacional actual, puso de manifiesto la existencia de programas de espionajes y de seguridad de información instrumentadas por este gobierno, lo cual fue cuestionado por la opinión pública al violar la soberanía de los estados y los derechos humanos de autoridades políticas y económicas, así como de los ciudadanos. Asimismo este caso demostró de manera documental la existencia de la diplomacia secreta norteamericana, así como las ventajas y limitaciones de dicha estrategia.

Los cables también pusieron a discusión en la opinión pública si la seguridad nacional norteamericana se encuentra por y sobre la soberanía extranjera y si sus estrategias para evitar posibles atentados terroristas pueden estar sobre la libertad de expresión y lo derechos de los ciudadanos a su privacidad.

El hecho de que la mayoría de los norteamericanos desconociera la existencia de bases de datos con información personal de funcionarios de otros países, pero también de ciudadanos norteamericanos abrió el debate sobre los límites del compromiso democrático del gobierno vs la seguridad nacional y sobre la falta de rendición de cuentas de las autoridades norteamericanas.

Por todas las razones anteriores utilizaremos el caso de Wikileaks como tema para analizar cuál fue la política de seguridad cibernética estadounidense de 2001 a 2013. El estudio del caso aportará a las relaciones internacionales un análisis de los programas instrumentados por este gobierno y las razones por las cuales no logró proteger la información clasificada a pesar de los filtros y resguardos de información utilizados, como el programa *International Strategy for Cyberspace,* Estrategia Internacional para el Ciberespacio. Mostraremos que los protocolos fueron insuficientes para lograr el resguardo de la información y que las Agencias de Inteligencia recurrieron a la subcontratación de empresas privadas, a las cuales se les permitió el manejo de información reservada, complicando aún más el proceso de resguardo de la información.

Analizaremos la autonomía excesiva en materia de ciberseguridad de las Agencias de Inteligencia norteamericanas, las cuales no le están rindiendo cuentas al Congreso sobre cómo utilizan su presupuesto, cuáles son las actividades y a qué personas están investigando. Incluso, no se conoce cómo protegen esta información y la forma en la que se utiliza. Amparándose en leyes como la Ley de Vigilancia de la Inteligencia Extranjera (FISC, siglas en ingles) de 2008 que brindaba a la Agenda de Seguridad Nacional (NSA, siglas en ingles) amplios poderes, los ciudadanos norteamericanos han padecido espionaje

telefónico y de correos electrónicos, lo cual viola la Cuarta Enmienda Norteamericana, por lo cual ahora se discute la legalidad de que este gobierno recabe metadatos de Internet, cómo los utiliza y cuáles son los mecanismos para evitar un inadecuado uso de información reservada.

Además reflexionaremos sobre el costo económico excesivo de esta política de seguridad, ya que el gobierno destina un alto porcentaje del presupuesto federal para las 16 Agencias Nacionales de Inteligencia con las que trabajaba el Departamento de Defensa.

Se analizarán también los efectos diplomáticos que tuvo Wikileaks y la diplomacia secreta norteamericana en países como México; Afganistán; Egipto; Argentina; Ecuador; Italia; Rusia; China; Corea del Norte. La difusión de los cables generaron fuertes reacciones en la opinión pública, pero sólo dos casos derivaron en un conflicto diplomático grave que implicó la reasignación o expulsión de los embajadores en México y Ecuador, lo cual fue un indicador de que la mayoría de los efectos fueron mediáticos más que diplomáticos.

Para analizar este tema se proponen las siguientes preguntas de investigación: ¿Qué implicaciones tuvo el 11 de septiembre de 2001, en las políticas de seguridad cibernética?, ¿Qué significó la filtración de los C*ablegates* en materia de políticas de seguridad cibernética para los Estados Unidos?, ¿Por qué las Agencias de Inteligencia de los Estados Unidos se vieran rebasadas e incapacitadas de mantener resguardada su información clasificada?, ¿Cuáles fueron las consecuencias para el gobierno norteamericano de la filtración de información clasificada por parte de los *Cablegates*?, ¿Cuál fue la reacción internacional y de la opinión pública sobre la revelación de esta información confidencial?, ¿Qué políticas instrumentó el gobierno de los Estados Unidos tras la filtración de información, para protegerse?

La hipótesis general de esta investigación será comprobar que desde el 11 de septiembre de 2001 la seguridad cibernética se convirtió en una prioridad para los

Estados Unidos en materia de seguridad nacional. Sin embargo, la filtración de información de los *Cablegates* evidenció el fracaso de estas políticas. Internamente se hizo evidente que los protocolos de seguridad no han sido eficientes, que las Agencias de Inteligencia no rinden cuentas y no tienen controles por parte del Congreso, ni del Presidente y que existe falta de regulación de corporaciones privadas en el manejo de información clasificada. Internacionalmente el caso evidenció la presencia de espionaje oculto por parte del gobierno norteamericano, lo cual generó fricciones diplomáticas y cuestionó la violación a la soberanía de otros países por parte de la opinión pública.

Las hipótesis secundarias que se intentarán comprobar en los cuatro capítulos de esta investigación serán las siguientes: el 11 de septiembre de 2001 marcó un cambio para las políticas de seguridad informática convirtiéndose en una prioridad nacional e internacional, incrementando el presupuesto dedicado a esta área. Se modificaron las competencias de las Agencias de Inteligencia orientadas al manejo de información reservada y se incrementó la subcontratación de empresas privadas, lo cual generó vicios en el sistema, protocolos insuficientes para mantener resguardada la información, adicionado a una sobresaturación de información.

Otra hipótesis secundaria que se pretende comprobar es que la filtración de información por parte de los C*ablegates* generó cuestionamientos hacia el desempeño de las autoridades norteamericanas, porque no rinde cuentas y tiene gastos excesivos en materia de seguridad informativa. La filtración de información generó que el gobierno de los Estados Unidos impulsara una restructuración administrativa en el manejo de la información, puso a discusión las relaciones entre las Agencias de Inteligencia y el débil papel del Congreso en el manejo de la política de seguridad informática.

A nivel internacional los C*ablegates* de Wikileaks pusieron en tela de juicio la labor diplomática y la política de espionaje que atenta contra la soberanía de los Estados en aras de priorizar la seguridad interna.

En el Capítulo 1 se reconoce que no existe hasta el momento una teoría dentro de la disciplina de las Relaciones Internacionales que ayude a analizar los conflictos y amenazas dentro de la red digital de Internet. Por lo que se intenta hacer una síntesis de algunos elementos teóricos de esta disciplina como el realismo, neorrealismo, liberalismo, neoliberalismo y constructivismo que pueden ser de utilidad para entender cuál es el papel de los Estados dentro de esta revolución tecnológica, la interacción entre Estados en esta nueva era digital y los problemas de seguridad que pueden enfrentar. También se realiza un análisis de los principales conceptos aplicados a lo largo de esta investigación para tener mayor claridad y evitar confusiones sobre el uso que se les dará a lo largo del trabajo.

En el Capítulo 2 se realiza un recuento histórico de las principales políticas en materia de seguridad cibernética instrumentadas en las dos últimas administraciones del gobierno de los Estados Unidos, desde 2001 tras los atentados terrorista hasta 2013. Es decir, en las administraciones de George W. Bush y Barack Obama. El propósito es dilucidar si hubo continuidad o diferencias en las políticas, así como conocer la dinámica que siguieron las actividades de inteligencia en estas dos administraciones.

De igual manera se realizar un análisis de los éxitos y fracasos de estas políticas de seguridad para de esta manera comprender cuáles fueron las debilidades y limitaciones que podrían explicar el por qué fue posible la filtración de información clasificada, en un país que le ha dado tanta importancia tanto a la Seguridad Nacional, como al ciberespacio y a las innovaciones tecnológicas.

En el Capítulo 3 se realiza un estudio de cuáles fueron las principales consecuencias internas que trajo para el gobierno norteamericano la filtración de los *Cablegates* por parte de Wikileaks en distintos niveles, en aspectos técnicos,

presupuestales y estructurales. Dentro de esas consecuencias encontramos la modificación de aspectos técnicos con el incremento de medidas de seguridad en los protocolos de las agencias de inteligencia, como una disposición para evitar futuras amenazas. Adicionalmente, se hace una revisión del incremento presupuestal que han tenido las agencias de inteligencia en los últimos años dentro del presupuesto federal. En este capítulo se hace un análisis sobre el funcionamiento de los Comités de Inteligencia del Congreso de ese país, analizando el por qué estos Comités no están cumpliendo con una verdadera supervisión de las actividades de inteligencia. De igual manera se analizan las razones por las que en los últimos años las agencias de inteligencia han incrementado la subcontratación de empresas privadas, para realizar tareas esenciales del gobierno y cuáles han sido sus consecuencias.

El Capítulo 4 se centrará en realizar un análisis de los principales cables diplomáticos revelados por Wikileaks, para de esta manera mostrar que muchos de ellos no tuvieron implicaciones diplomáticas, a pesar de que algunos temas abordados son delicados y fueron cuestionados por la opinión pública. Es por esta razón que también se realiza un análisis de las posturas tanto a favor como en contra por parte de la opinión pública y las críticas que realizaron sobre el constante espionaje y violación a Derechos Humanos por parte del gobierno de los Estados Unidos.

Capítulo 1 Marco teórico-conceptual.

1.1. Marco teórico.

Actualmente, el papel de la tecnología en las relaciones internacionales es cada vez más evidente tanto para los Estados y como para las sociedades. La presencia de Internet ha modificado la dinámica informativa en distintos niveles tanto en la dinámica internacional, como estatal, social, económica, cultural, etc. Ello ha significado un cambio significativo, en donde se rompen las barreras físicas que prevalecían en el pasado y el modo de interacción entre Estado y sociedad y entre la sociedad misma.

El Internet ha tenido una rápida evolución, pasando de ser un mecanismo dominado por las élites políticas y económicas a uno de comunicación masiva, en donde cualquier persona que cuente con una computadora y acceso a la red puede establecer comunicación con cualquier parte del mundo de manera casi simultánea, ello ha incrementado la popularidad de este medio y su acelerada expansión por el mundo.

El Internet y las comunicaciones dentro de la red se han vuelto cada vez más comunes, han ayudado a generar procesos más efectivos y productivos en distintas áreas de la vida tanto política, social y económica. Ello llevó a pensar que era un medio seguro para establecer contacto con otros individuos y para guardar información. Sin embargo, esta aseveración es una falsa consideración, ya que el Internet fue diseñado para maximizar y simplificar las comunicaciones, no para proteger estas comunicaciones, por lo cual se vuelve tarea de los Estados asegurar la información que circula en Internet para evitar esta vulnerabilidad de la red, que pone en peligro a las sociedades que se encuentran conectadas.

En este contexto, surge un dilema relacionado con la ciberseguridad, que pone en evidencia no solamente la protección de los sistemas informáticos, sino cuestiona si el Estado tiene la capacidad soberana para controlar la información que circula

en su territorio nacional. Esto ha llevado a pensar que el ciberespacio se ha convertido en el nuevo campo de batalla entre Estados y actores no estatales. Y por tal razón la vieja concepción de seguridad, entendida como enfrentamiento bélico ha cambiado adquiriendo connotaciones más amplias que incluyen el aspecto cibernético.

En virtud de lo anterior, deriva la importancia de hacer un análisis de esta nueva realidad internacional. Para ello, se tomarán en consideración posturas teóricas como el realismo, neorrealismo, liberalismo, neoliberalismo y constructivismo, así como de la opinión pública. La razón de esta variada revisión teórica obedece al hecho de que hasta el momento no existe aún una teoría dentro de las relaciones internacionales que aborde de manera específica los conflictos cibernéticos dentro de la sociedad internacional actual. Tampoco existen respuestas claras sobre ¿cuál es el papel que tienen los Estados dentro de esta revolución tecnológica? y ¿cuáles son las implicaciones para la seguridad, tanto nacional como internacional, de esta revolución?

Dentro del paradigma del realismo político desarrollado principalmente por Hans Morgenthau[1] se argumenta que los Estados son los actores más importantes de la política mundial, los cuales responden a un comportamiento racional. Buscan obtener el poder, preservar su interés nacional para de esta manera conseguir sus objetivos dentro de un mundo anárquico basado en el principio de la naturaleza conflictiva de las relaciones internacionales[2]. Esta premisa es abordada por Thomas Hobbes, quien en su obra *El Leviatán* hace referencia a la tarea primordial del Estado de preservar la integridad de sus ciudadanos y librar al individuo de las incertidumbres del mundo anárquico. Alude no solamente a

[1] El pensamiento de Morgenthau hace referencia a que la política está regida por la naturaleza humana que es formulada de manera racional. Los Estados se mueven a través de la búsqueda del interés en términos de poder, Véase "Biografía Hans Morgenthau", *Boletín de Relaciones Internacionales,* Núm. 5, Agosto-Septiembre 2004, Dirección URL: http://nortecity.com.ar/relinter/numero5_pagina5.html, [Consultado el 18 de noviembre 2013].

[2] Esther Barbé (1987): "El papel del realismo en las relaciones internacionales. La teoría de la política internacional de Hans J. Morgenthau", Revista de Estudios Políticos, No. 57, p. 154.

garantizar la vida, sino también a la importancia de que prevalezca la estabilidad social, donde el conflicto pueda ser resuelto a través de la intervención estatal. Bajo esta premisa los autores realistas consideran que el Estado deberá ser el encargado de proteger la seguridad de los individuos[3], pero para lograrlo requiere de poder político, ello ha sido definido como: "tanto el interés nacional como el deseo de supervivencia precisan para su logro de la seguridad y ésta depende del poder que se posee"[4].

La escuela realista de la Seguridad Nacional asevera que las acciones de inteligencia son una herramienta para preservar los intereses de la nación y del Estado. Sin embargo, esta interpretación privilegia la defensa militar y la política exterior, siendo las Agencias de Inteligencia los ejes de la ejecución de estrategias para evitar amenazas y riesgos contra el Estado[5]. Es por ello que este enfoque es de utilidad para esta investigación ya que nos ayudara a entender la vinculación entre dichas agencias de inteligencia y la política de seguridad dentro del ciberespacio.

La visión neorrealista puede ser también de utilidad para entender nuestro objeto de estudio, ya que de acuerdo con Kenneth Waltz[6], en su libro "Teoría de la Política Internacional", el comportamiento de los actores está determinado por el sistema, el cual consiste en estructuras organizadas donde interactúan unidades. El sistema nace de la actividad de los Estados cuyos objetivos y esfuerzos están concentrados en satisfacer sus propios intereses de poder y seguridad. Razón por lo cual el sistema es anárquico, dinámica que conduce a que los Estados estén en una constante preparación para una posible guerra. Esto hace referencia a las

---

[3] Carlos Miranda, "Hobbes y la anarquía internacional", *Revista de Ciencias Políticas*, Núm. 2, Vol. VI, Chile, 1984, pp.73 y 74.
[4] Carlos Miranda, "Realismo e idealismo en el Estadio de las Relaciones Internacionales: la influencia de Hobbes y de Kant", *Revista de Ciencia Política*, Chile, Núm. 95, Vol. VIII, 1986, p. 92.
[5] "Inteligencia y seguridad", *Revista de análisis y prospectiva*, España, Ed. Universidad Rey Juan Carlos y Universidad Carlos III de Madrid, Núm. 4, Julio-noviembre 2008, p. 34.
[6] Politólogo estadounidense (1924-2013) creador del realismo estructural.

interacciones entre Estados las cuales se ven afectadas por límites y la distribución de capacidades dentro del sistema[7].

A diferencia del realismo tradicional el neorrealismo en primer lugar se apoya en la teoría económica, no en la sociología e historia como es el caso del realismo, aunado a ello el neorealismo "contempla el poder como un medio". La preocupación que guía a los Estados no es el poder, sino la seguridad"[8], lo que lleva a éstos a mejorar sus tecnologías para incrementar sus instrumentos de fuerza. Es decir, que los Estados lejos de buscar crear estructuras o maximizar el poder, buscan asegurar su supervivencia. En esta teoría Waltz plantea que el sistema político internacional está formado por el principio de auto-ayuda, esto quiere decir que los Estados dependen de sus propias acciones para enfrentar las amenazas de una guerra[9].

Una visión más reciente de esta corriente la da James Adams en su artículo *Virtual Defenses*[10] en el cual plantea que el Internet es un sistema anárquico, donde "el ciberespacio se ha convertido en un nuevo campo de batalla internacional"[11], que no tiene un cuerpo que la gobierne o vigile. Ello provoca que cada Estado se vea obligado a crear fuerzas cibernéticas y de defensa de la seguridad en esta materia, ya que una amenaza directa a su infraestructura critica afectaría su propia seguridad.

---

[7] Mónica Salomón González, "La Teoría de las Relaciones Internacionales en los albores del siglo XXI, dialogo, disidea, aproximaciones" *Revista CIDOB d'Afers Internacionals***,** Núm. 56, Barcelona, España, 2003, p.14.
[8] Kepa Sodupe, *La teoría de las Relaciones Internacionales a comienzos del Siglo XXI*, España, Ed. Universidad del País Vasco, 2003, p.81.
[9] *Ibid.*, p. 88.
[10] Este artículo con una visión neorrealista parte de la idea de explicar cómo a pesar del gran poderío militar y nuclear los Estados Unidos tras el fin de la Guerra Fría se encuentran vulnerables frente a un ciberataque, debido a que las fuerzas militares se volvieron cada vez más dependientes de las tecnologías informáticas, por lo que se han vuelto una nueva arma que pueden utilizar los países enemigos en contra de los Estados Unidos. Esto se puede ver reflejado en varios ataques cibernéticos que ha tenido este gobierno como el caso Moonlight Maze (ataque a la red de la NASA por hackers rusos).
[11] James Adams, "Virtual Defense", *Revista Foreign Affairs*, Estados Unidos, Núm. 3, Vol. 80, (May-Jun., 2001), p. 98.

Esta escuela explica también la naturaleza alarmante del dilema de seguridad, en donde estas nuevas amenazas cibernéticas representan un reto para el estudio de las relaciones internacionales porque parte del supuesto que un Estado puede atacar a otro en el ciberespacio sin ser descubierto y con total impunidad. Esta teoría predice que habrá un colapso total de la confianza entre los estados y los organismos internacionales, ante el temor de ataques, generando la necesidad a nivel estatal de contar con fuerzas de defensa cibernéticas.

Tanto para el realismo como para el neorrealismo la seguridad implica conservar la integridad territorial del Estado, para proteger los intereses de la nación y mantener el bienestar de la sociedad. Razón por la cual ambas teorías hacen referencia a la necesidad de los Estados de contar con los medios necesarios para preservar ese interés nacional y sobrevivir dentro de este sistema anárquico. Sin embargo, la corriente neorrealista tiene como limitante el no tomar en consideración a otros actores no gubernamentales, como es el caso de Wikileaks. Si bien los Estados pueden ser considerados como los principales actores en una batalla cibernética gracias a sus capacidades financieras y tecnológicas, también existen otros grupos que desempeñan un papel relevante, tal es el caso de los grupos de interés, organizaciones terroristas e individuos claves que pueden causar daños a la seguridad informática de los Estados. Esta teoría hace referencia a la existencia de una gran interdependencia dentro de las redes digitales, lo cual genera un incremento de la vulnerabilidad de la soberanía de los Estados.

Por su parte, la teoría liberal acepta que se ha incrementado la pluralidad y relevancia de los actores no estatales, con capacidades transnacionales de presión, actores que han adquirido cada vez más importancia, gracias al incremento de organizaciones internacionales, de grupos terroristas, individuos y grupos de poder que interactúan y actúan dentro del ciberespacio.

Para ejemplificar esta teoría recurriremos a Emmanuel Kant considerado un liberal dentro de las relaciones internacionales por su postura frente a la seguridad, según la cual la principal competencia del Estado es el proteger los derechos inalienables de sus ciudadanos, para lo cual se deben crear ordenamientos jurídicos internacionales. Sin embargo, a diferencia de Hobbes, Kant plantea que se deben crear instituciones internacionales para regular las acciones del Estado y evitar llegar a una guerra y poner en ejercicio los imperativos morales que limitan al Estado, para lograr la paz perpetua. Estableciendo leyes para limitar la guerra y acciones de cooperación para lograr una seguridad colectiva, lo que llevará a generar una confianza mutua entre los Estados[12].

Otra teoría que puede ser de utilidad para esta investigación es la corriente neoliberal representada principalmente por Robert Kehoane tiene como principal propósito lograr un mundo en condiciones de paz, bienestar y justicia a través de la cooperación internacional. Se basa no sólo en la presencia de Estados como actores, sino también en la cooperación de actores racionales que buscan alcanzar el poder y lograr influencia a través de la cooperación[13]. Esta corriente también destaca la relación entre el sector público y el privado para proveer servicios. Se reconoce que los gobiernos de manera autónoma no pueden proporcionar la gran cantidad de servicios públicos que necesita las sociedades modernas, teniendo que acudir a los privados. Esta postura en un principio se aplicó a los sectores de la salud, educación y trasporte. Sin embargo, se ha extendido a otros sectores como la seguridad nacional. Un ejemplo de la relación público-privado en el gobierno de los Estados Unidos es la Estrategia Nacional para la Seguridad del Ciberespacio de la Junta de Protección de la Infraestructura

---

[12] Teresa Santiago Oropeza, "Kant y su proyecto de una paz perpetua", *Revista Digital Universitari, [en línea]*, Núm. 11, Vol. 5, Ed. UNAM, México, 10 de diciembre 2004, Dirección URL: http://www.revista.unam.mx/vol.5/num11/art77/dic_art77.pdf, p. 6, [Consultado el 10 de noviembre 2013].

[13] Mónica Salomón González, *op. cit*., p.52.

Crítica del presidente Bush de septiembre de 2002 basada en asociación público-privada, admitiendo que "el Gobierno solo no puede asegurar el ciberespacio"[14].

Extrapolando este concepto podría pensarse que los estados seguirían en el ciberespacio una política de cooperación. Sin embargo, la cooperación parece un reto difícil de alcanzar, ya que todos los estados son vulnerables dentro de la red, pero si prevalece una dinámica público-privada los riesgos se incrementan porque es aún más complicado lograr un control en el ciberespacio.

Otra teoría que brida aportes a nuestro tema de estudio es una rama de la teoría constructivista, llamada la "*securitización*" desarrollada por la Escuela de Copenhague[15] específicamente por Waver. Esta teoría destaca la manera en la que se construye la agenda de seguridad a través de los mensajes políticos de actores claves. Ello se convierte en un medio para legitimar medidas como el uso de la fuerza, la invasión de la privacidad en aras de mantener la estabilidad de los Estados. Sin embargo, esta postura no ha hecho alusión específica a la ciberseguridad, pero su interpretación es de ayuda para entender la dinámica actual que se vive en el ciberespacio.

Como podemos ver todas estas posturas teóricas si bien tiene alguna relación con la temática a analizar, ninguna está especializada en el tema. La teoría realista aboga en torno a la fuerza del estado para proteger su soberanía. Mientras que la teoría neorrealista pone énfasis en la importancia de que la guerra puede ser informática y la innovación tecnológica se ha convertido en un área estratégica que debe defenderse. En contraste el aporte de la corriente liberal, para nuestro,

---

[14]Johan Eriksson y Giampiero Giacomello, "Information Revolution, Security, and International Relations; (IR) relevant Theory?" *International Political Science Review*, Núm. 3, Vol. 27, Ed. Sage Publications, 2006, p. 231.

[15] Teoría que hace referencia al proceso discursivo en la comunidad política para controlar algún objeto que se convertirá en una amenaza existencial para lo cual se necesitan genera medidas para contrarestarla. Véase Úrsula Oswald Spring y Hans Gunter Brauch, *Reconceptualizar la seguridad en el siglo XXI, [en línea]*, México, UNAM, 2009, pp. 283, Dirección URL: http://www.crim.unam.mx/drupal/?q=node/407, [Consultado el 15 de noviembre 2013].

estudio es el nuevo papel que tiene los actores no estatales, mientras que la corriente neoliberal destaca la asociación pública y privada en sectores estratégicos como la seguridad, así como la importancia de la cooperación internacional para mantener la paz mundial.

Finalmente, la teoría de la *securitización* es de utilidad para entender primero los discursos políticos en materia de seguridad así como la manera en la que se construye la agenda política.

Estas teorías nos ayudarán a entender cuál es la importancia que tiene para los Estados el establecimiento de políticas de seguridad que regulen el ciberespacio, para de esta manera prevenir y evitar una amenaza a la seguridad nacional.

Para esta investigación necesitamos no sólo la visión estatal sobre este problema, sino entender el papel de la opinión pública, ya que será ella la que evidencie las debilidades que prevalecen en las políticas de ciberseguridad instrumentadas por el gobierno norteamericano. La opinión pública se ha convertido en una actor clave a nivel internacional por su influencia en otros actores que pueden ser determinantes en la toma de decisiones.

El concepto de la opinión pública surgió de la Ciencia Política, donde no existe una única definición[16]. Sin embargo, la mayoría de ellas hacen referencia a que la opinión pública engloba la noción de opiniones o juicios expresados en contra o a favor de algún tema, que pueden basarse en predisposiciones emotivas o racionales. Encontramos los orígenes de la idea de opinión pública desde la

[16] Por una parte David Hume plantea que la opinión pública implica un proceso de integración del que dependen también los gobernantes. Otra postura es la de Robert Merton quien en su libro Social Theory and Social Structure, plantea que "la opinión pública forma parte del discurso racional entre ciudadanos informados y responsables, con el fin de orientar la opinión y la toma de decisiones en una democracia" Elisabeth Noelle-Neumann, "La espiral del silencio. La opinión pública y los efectos de los medios de comunicación", *Revista Comunication & Society*, Universidad de Navarra, Núm. 1. Vol. VI, 1993, Dirección URL: http://www.unav.es/fcom/comunicacionysociedad/es/articulo.php?art_id=226, [Consultado el 18 de noviembre 2013].

filosofía política de Locke[17], Rousseau[18] y Jeremy Bentham, pero se utiliza el concepto de opinión pública como tal hasta el siglo XVIII, haciendo referencia a juicios colectivos más allá de la esfera del gobierno que afectaba la toma de decisiones políticas.

La disciplina de las relaciones internacionales ha adoptado este concepto denominándolo "opinión pública internacional", la cual fue estudiada por Rafael Calduch en su libro *Relaciones Internacionales,* donde considera que es "una forma de agrupación social constituida por individuos o colectividades de distintos países que adquieren imágenes, generales o particulares, y realizan valoraciones comunes sobre los acontecimientos internacionales a partir de la información recibida por su inserción en flujos trasnacionales de comunicación"[19].

Para este autor la gran cantidad de fuentes comunicativas y las informaciones trasmitidas generan una gran pluralidad de opiniones, de públicos y de movilización lo que dificulta su análisis como un actor homogéneo porque "hablar de opinión pública internacional como un grupo de presión más que como un actor internacional plenamente estructurado en su interior y definido en las formas de actuación exterior"[20].

La opinión pública si bien es un actor determinante, no llega a equipararse con los demás actores del sistema internacional (Estados, Organizaciones

---

[17] John Locke planteaba que la opinión pública ejerce una gran presión la cual se vuelve muy difícil de resistir.

[18]Jean Jacques Rousseau en su libro El contrato social "La opinión pública, un factor que desconocen nuestros teóricos de la política, pero del que depende el éxito de todo lo demás" Véase Jean Jacques Rousseau, "The Social Contract" (l792), in *Political Writings,* Londres, 1953, p. 58. En Elisabeth Noelle-Neumann, "La espiral del silencio. La opinión pública y los efectos de los medios de comunicación", *Revista Comunication & Society*, Universidad de Navarra, Núm. 1. Vol. VI, 1993, Dirección URL: http://www.unav.es/fcom/comunicacionysociedad/es/articulo.php?art_id=226, [Consultado el 18 de noviembre 2013].

[19] Rafael Calduch, Relaciones Internacionales, Capítulo 13 El público, la opinión pública y la sociedad internacional, Edit. Ediciones Ciencias Sociales, Madrid, 1991, p. 349.

[20] *Ibid.,* p. 350.

Internacionales, trasnacionales), sino que solo se queda en el terreno de los actores de presión e influencia y no de toma de decisiones.

Rafael Calduch también considera que la opinión pública internacional es diferente a la opinión pública nacional, ya que la internacional tiene mayor eficacia y mayores alcances, porque puede influir en personas de diversos países y tener peso en los gobiernos. Uno de los principales actores de la opinión pública internacional son los líderes de opinión, los cuales surgen de los apoyos que obtienen en las poblaciones. Ejercen una presión sobre el público y sobre los gobiernos de los países o influyen en su comportamiento.

Por otra parte, Marcel Merle en su libro *Sociología de las Relaciones Internacionales*[21]*,* plantea que la opinión pública internacional es producto de los diferentes puntos de vista de las opiniones nacionales, las cuales pueden tener distintos orígenes, ya sea gobierno, medios de comunicación masivos, o grupos de presión. Esta opinión pública surge como producto de la existencia de acontecimientos, los cuales generan una postura común que se refleja en pronunciamientos y opiniones. Es decir, esta opinión pública internacional "es el producto o la resultante de las tensiones dialécticas que se manifiestan en las relaciones entre: 1) cada gobierno y su propia opinión pública; 2) la colectividad de gobiernos y el conjunto de las fuerzas que luchan a favor de una transformación del sistema internacional"[22].

Sin embargo, Merle tiene algunas reservas que debemos considerar al momento de analizar la opinión pública internacional, ya que considera que, "la expresión de una opinión, aunque sea solamente y ampliamente mayoritaria, no garantiza la conformidad de los comportamientos"[23]. Lo que significa que se debe tener

---

[21]Marcel Merle, Sociología de las relaciones internacionales, España, Ed. Alianza Universitaria, 1978, Pp. 379-393.
[22] *Ibid*., p. 390.
[23]*Ibid.*, p. 382.

cuidado al analizar la opinión pública, ya que aunque pueden llegar a consensos y acuerdos sobre algún tema esto no garantiza que al momento de actuar sigan estos principios.

Otro autor que ha estudiado la opinión pública internacional es José Escribano quien plantea que está surge de la convergencia entre las opiniones públicas, que puede darse por tres maneras. La primera surge de la coincidencia de representantes de los gobiernos que llegan a acuerdos dentro de las Organizaciones Internacionales, los cuales generan tendencias regionales que se convierten en principios gracias a los consensos entre los representantes e influyen en los actores oficiales. Una segunda opción es que la opinión pública puede surgir del consenso de las diversas opiniones públicas nacionales sobre algún problema, lo cual no significa que sean idénticas o semejantes. Y por último este autor considera que puede surgir de corrientes de opinión que tengan una misma base ideológica o política[24].

Debido a su capacidad de presión política, podríamos considera que este nuevo sujeto de las relaciones internacionales ha adquirido relevancia en la sociedad internacional y en los representantes gubernamentales, convirtiéndose en un actor clave a estudiar en esta investigación. La opinión pública fue determinante para analizar las implicaciones de las políticas de espionaje e inteligencia que se revelaron con los *Cablegates* del Departamento de Estado de los Estados Unidos.

[24] José Escribano Úbeda-Portugués, *Lecciones de Relaciones Internacionales*, Ed. Aebius, Madrid, 2010, pp. 111-112.

1.2 Marco conceptual

Para iniciar la investigación es pertinente hacer un análisis de los diferentes conceptos fundamentales que se incluyen a lo largo de esta investigación con la finalidad de ser precisos y no generar confusiones.

1.2.1 La Seguridad para los Estados Unidos.

El concepto de seguridad es una noción clave para nuestro estudio. Sin embargo, es preciso subrayar que tiene distintos significados y puede ser utilizado en diversos ámbitos de análisis, puede hablarse de seguridad humana, seguridad energética, seguridad jurídica, seguridad financiera, seguridad nacional, ciberseguridad, entre otras, y nos concentraremos en esta última para la investigación.

La noción clásica de la seguridad dada por la escuela realista, representada principalmente por Hans Morgenthau[25] y Kenneth Waltz[26] plantea que en el sistema internacional los Estados son los actores principales, los cuales buscan sus propios intereses para ejercer el poder. Es por ello que "la seguridad nacional generalmente se entiende en términos de los recursos a disposición del poder –principalmente militares- y esta defensa usualmente se coloca en la cúspide de la

[25] Teórico realista de gran influencia dentro de la academia estadounidense durante el periodo de entre guerras durante la primera mitad del siglo XX. Exiliado de Alemania a los Estados Unidos en la Segunda Guerra Mundial, perteneció al Comité de Planeación Política del Departamento de Estado y asesor del Departamento de Defensa estadounidense. Véase: Biografía Hans Morgenthau, *Boletín de Relaciones Internacionales*, Núm. 5, Agosto-Septiembre 2004, Dirección URL: http://nortecity.com.ar/relinter/numero5_pagina5.html, [Consultado el 20 de noviembre 2013].

[26] Teórico de las relaciones internacionales de gran influencia en el periodo de post Guerra Mundial, se le asocia con la teoría neorrealista o estructural por su libro *Theory of Internaional Politics*. Véase: Jo Jakobsen, Relations-Kenneth Waltz, Popular Social Science, Dirección URL: http://www.popularsocialscience.com/2013/11/06/neorealism-in-international-relations-kenneth-waltz/ [Consultado el 27 de noviembre 2013].

escala de prioridades de los estados-nación"[27]. Es decir, este modelo hace referencia al importante papel del Estado como encargado de la seguridad de la sociedad, el interés nacional y que también tenga la fuerza para proteger sus intereses legítimos y enfrentar la amenaza de otros Estados.

La elección de esta escuela indica que el gobierno norteamericano, objeto principal de nuestro estudio, adoptó la postura realista después de la Segunda Guerra Mundial, por ser una herramienta teórica que se adaptaba a sus condiciones de postguerra e ideología. Esto ocurrió debido al hecho de que después de esta guerra, los Estados Unidos contaban con un gran poder económico y una gran capacidad militar, que les permitió convertirse en una potencia global. Para lograr esto el gobierno de Harry S. Truman creó la Ley de Seguridad Nacional (*National Security Act*)[28] que fue el esquema para el establecimiento de instituciones gubernamentales dedicadas a preservar la seguridad del Estado, como fue el caso del Consejo de Seguridad Nacional, donde se establecieron todas las normas militares y el surgimiento de la Agencia Central de Inteligencia (CIA, siglas en ingles), encargada de las actividades de inteligencia de los Estados Unidos y de la evaluación y diseminación de lo que afecta a la seguridad nacional[29].

Para los Estados Unidos hablar de seguridad, era sinónimo de Seguridad Nacional y la principal función del Estado soberano era garantizar la paz a través del ejercicio del poder, preservando los intereses nacionales frente a cualquier amenaza. Por tal razón las políticas de seguridad nacional tienen como prioridad

---

[27] Sergio Aguayo Quezada y Michael Bagley Bruce, *En busca de la Seguridad Pérdida, Aproximaciones a la seguridad nacional mexicana,* México, Ed. Siglo XXI, 2002, p. 19.

[28] Esta Acta de Seguridad Nacional significó una reorganización de la política exterior y la política militar para los Estados Unidos unió al Departamento de Marina y al Departamento de Guerra, que se unieron para crear el Departamento de Defensa bajo el mando del Secretario de Defensa o *National Security Council* (NSC). También se creó el Departamento de la Fuerza Aérea, y el Consejo de Seguridad Nacional (NSC). Véase: National Security Act of 1947, Department of State, Office of the Historian, Dirección URL:http://history.state.gov/milestones/1945-1952/national-security-act,[Consultado el 21 de noviembre 2013].

[29]Véase. Historia de la CIA, Central Intelligence Agency, [en línea], Dirección URL: https://www.cia.gov/es/about-cia/history-of-the-cia, [Consultado el 21 de noviembre 2013].

la formulación e instrumentación de estrategias nacionales que incluyen la amenaza o el uso de la fuerza para crear un ambiente propicio para los intereses nacionales de los Estados Unidos[30].

Para este país la seguridad nacional tiene estrecha relación con los intereses nacionales que pueden ser intereses vitales, tal como la protección del territorio, para lo cual requiere la movilización de recursos militares. También puede responder a intereses críticos, los cuales no afectan directamente las áreas vitales, pero podrían convertirse en el futuro en estratégicos y finalmente, podríamos señalar que existen los denominados intereses serios, los cuales no afectan los dos antes referidos, pero no por ello pierden relevancia[31].

A pesar de que la definición clásica de seguridad es de gran importancia para este trabajo, es necesario tomar en cuenta que actualmente estamos transitando hacia una nueva época en la que este concepto integra amenazas nuevas y antiguas, y las considera de una manera diferente. Esto es debido al acelerado desarrollo de las tecnologías, amenazas al medio ambiente, terrorismo, crisis financiera, y demás situaciones que contrastan con valores tales como desarrollo humano, convivencia democrática, búsqueda de paz, protección de derechos humanos, etc. En este contexto, las amenazas ya no provienen solamente de acciones político-militares sino de otras fuerzas que han adquirido mayor poder a nivel internacional y cuyo control rebasa el ámbito estatal.

---

[30]Texto original en ingles: "*National security policy is primarily concerned with formulating and implementing national strategy involving the threat or use of force to create a favorable environment for US national interests*". Sam C. Sarkesian, Allen Williams John y Stephen J. Cimbala, *US National Security: Policymakers, Processes & Politics,* Estados Unidos, Ed. Lynne Rienner Publishers, 2008, p. 5.

[31] Sam C. Sarkesian, Allen Williams John y Stephen J. Cimbala, *U.S. National Security Policymakers, processes and politics,* Estados Unidos, Ed. Lynne Rienner publishers, 2002, p.13, en Tesis Méndez de la Brena Dresda Emma, Licenciatura en Relaciones Internacionales, Universidad de las Américas Puebla, Escuela de Ciencias Sociales, Artes y Humanidades, 2006, p. 23.

En suma el concepto de seguridad ha evolucionado conforme a la trasformación de las nuevas amenazas contra la Seguridad Nacional. El acelerado avance tecnológico ha contribuido a acelerar los procesos de comunicación, la trasferencia de mercancías, la eliminación de barreras y fronteras físicas, pero también ha propiciado que los aspectos tecnológicos sean ahora parte de las estrategias de seguridad de los Estado y por ello es importante analizar el concepto de ciberseguridad.

1.2.2 Ciberseguridad

Antes de analizar la llamada ciberseguridad debemos reflexionar sobre el concepto de "ciber" el cual surgió en 1948 con los trabajos de Norbert Wiener, quien planteó el término cibernética en su libro *Control y Comunicación en el animal y en la máquina*[32]*.* El concepto de "ciber" puede hacer referencia a varios aspectos de la informática, se puede hablar de ciberseguridad, ciberespacio, ciberamenaza, ciberterrorismo, ciberguerra, entre otros. Pero para esta investigación solo nos centraremos en el concepto de ciberseguridad y ciberespacio.

Esta noción de seguridad cibernética o ciberseguridad tiene relación directa con el proceso de dominio territorial de los estados que implica no sólo cuidar la dimensión terrestre, marítima, aérea y espacial, sino incorporar una nueva dimensión: el ciberespacio. Si bien esta última no es un elemento tangible representa un importante riesgo para la seguridad de los Estados, porque se encuentra interconectada y las posibles amenazas no se observan a simple vista. Es por ello que la política de seguridad del ciberespacio requiere organización, un

[32] Norbert Wiener afirma que la cibernética es la ciencia del control y la comunicación entre el animal y la máquina, por lo cual es una ciencia multidisciplinaria. Por tal razón considera a la cibernética como un paradigma que explica los conceptos de las ciencias materiales, como estructura lógica-formal cuyo axioma es que los fenómenos del universo son consecuencia de un proceso de comunicación. Larisa Burtseva, Valentyn Tyrsa, Brenda Leticia Flores Ríos, *Norbert Wiener: Padre de la cibernética*, UABC, Mexicali, Abril-Junio 2006, Dirección URL: 132.248.129.5/cursoOJS/index.php/uabc/article/download/857/863, [Consultado el 24 de noviembre 2013].

entrenamiento y un equipamiento para controlarlo, lo que implica crear estructuras institucionales y profesionales capacitadas para enfrentar los retos que este nuevo dominio pueda presentar.

La ciberseguridad modifica el concepto de seguridad que prevalecía en el pasado e implica la gestión de riesgos para proteger los dispositivos informáticos en el ciberentorno. Podemos decir que "la ciberseguridad garantiza que se alcancen y mantengan las propiedades de seguridad de los activos de la organización y los usuarios contra los riesgos de seguridad correspondientes en el ciberentorno"[33].

Una amenaza a la ciberseguridad puede afectar no solo el bienestar de las sociedades, países o empresas, sino que también puede afectar la esfera política, social, económica, legal, diplomática, técnica, por lo cual es de vital importancia crear estrategias que sean efectivas y coherentes con las políticas y los principios de los países, lo cual ha impuesto nuevos retos a los Estados en torno a la creación de un marco normativo y regulatorio.

Debemos destacar que esta ciberseguridad no solo está diseñada para responder ante amenazas de Seguridad Nacional, sino que también se convierte en una condición necesaria para que la información tanto gubernamental como la empresarial, la tecnológica, etc. esté resguardada y no sufra alteraciones ni robos. Por ello se han creado medidas de protección[34].

El concepto de ciberseguridad como parte de la agenda de seguridad de los Estados comienza a adquirir relevancia a partir de los 90's. Se orienta a proteger la infraestructura crítica, vital para la seguridad nacional, debido a que se

---

[33]María José Caro Bejarano, "Alcance y ámbito de la seguridad en el cibeespacio", en *Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio*, Cuadernos de Estrategia, Ministerio de Defensa de España, España, Febrero 2011, p. 55.

[34] La amenaza de tácticas de <infoguerra> ya ha provocado la atención creciente hacia medidas de seguridad y protección, como muros de protección alrededor de los datos" Red Whitaker, *El fin de la privacidad. Cómo la vigilancia total se está convirtiendo en realidad*, España, Ed. Paidos, 1999, p.94.

empezaron a advertir vulnerabilidades en los Estados producto de la presencia de la tecnología y la globalización, que llevó a superar en la práctica las fronteras territoriales.

Con el acelerado acceso a las redes de Internet los riesgos se incrementaron, ello llevó a establecer lazos de cooperación entre el sector privado y el sector gubernamental frente a las amenazas de perder control en el manejo de información. Ello implicó el surgimiento de acuerdos para establecer una responsabilidad compartida que se vieron reflejadas en las políticas de ciberseguridad a las cuales haremos alusión a continuación.

1.2.3 Políticas de Ciberseguridad

El avance de las tecnologías han evidenciado que los Estados deben instrumentar políticas, adaptar medidas y controles que permitan proteger las redes informáticas y el ciberespacio para evitar cualquier ataque cibernético que pueda afectar la estructura gubernamental o empresarial, para lo cual el gobierno debe establecer normas técnicas y estándares nacionales e internacionales para proteger la infraestructura crítica de los Estados a través de políticas.

Para llevar a cabo políticas de ciberseguridad eficientes se debe lograr una coordinación entre los distintos sectores institucionales del Estado, por lo cual las políticas de ciberseguridad y la seguridad nacional se convierten en ámbitos complementarios, dado que ambos buscan liberar del peligro al Estado.

Sin embargo, estas dos nociones difieren en los actores que involucran y en el objeto de protección y para aclararlo iniciaremos señalando que la ciberseguridad busca asegurar los flujos de información dentro de Internet, mientras que la seguridad nacional incluye ámbitos más amplios como el manejo de las fuerzas armadas, de los servicios de inteligencia y medidas de defensa civil.

A pesar de que tienen diferencias conceptuales, la incorporación de la definición de seguridad cibernética dentro de la agenda política de los Estado ha hecho que estas dos nociones se interrelacionen.

Finalmente, es importante señalar que para crear políticas de ciberseguridad efectivas los gobiernos deben analizar diferentes elementos como son el político, el diplomático, el informativo, el militar y el económico, lo cual convierte a las ciberestrategias en una área que requiere de una postura. Es decir, se convierte en un tema estratégico que rebasa las nociones con las fue concebida esta política, porque en la práctica un mal ejercicio de las políticas de ciberseguridad podrían afectar al propio Estado.

1.2.4 Ciberespacio

El concepto de ciberespacio es analizado desde diversas perspectivas. Podemos encontrar definiciones muy simples como la de la Real Academia Española que define al ciberespacio como el "Ámbito artificial creado por medios informáticos"[35], que hace referencia a un medio no físico. Existen otras más amplias como la de la comunidad de Tecnologías de la Información y Comunicaciones (TIC) que "se refiere al conjunto de medios físicos y lógicos que conforman las infraestructuras de los sistemas de comunicaciones e informáticos"[36]. Otra definición dada por el Doctor Rain Ottis[37] es que el ciberespacio es "un conjunto de sistemas de información interconectados, dependientes del tiempo, junto con los usuarios que interactúan con otros sistemas"[38].

---

[35]Véase, Ciberespacio, Real Academia de la Lengua Española, Dirección URL:http://lema.rae.es/drae/?val=ciberespacio, [Consultado el 26 de noviembre 2013].

[36] Enrique Fojón y Ángel Sanz, *Ciberseguridad en España: una propuesta para su gestión*, Análisis del Real Instituto Elcano, ARI No. 101/2010

[37] Profesor de seguridad cibernética de la Universidad de Tecnología de Tallín Estonia y trabajó en el Centro de Defensa Cibernética Cooperativa de Excelencia de la OTAN.

[38] Ottis Rain and Peeter Lorents, Cyberspace: Definitions and Implications, Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia. 2010.

Sin embargo, tomando en consideración nuestro objeto de estudio utilizaremos la del Departamento de Defensa de los Estados Unidos, quien define al ciberespacio como "el dominio global dentro del entorno de la información consistente en la interdependencia de la red de infraestructuras de tecnologías de la información, que incluye el Internet, las redes de telecomunicaciones, sistemas de computadoras, procesadores y controladores de sectores críticos"[39].

Este ciberespacio es operado por actores estatales y privados que pueden ser amenazados desde cualquier parte del mundo en donde se tenga acceso al ciberespacio, por tal razón, desconoce fronteras, por lo que podemos decir que es la esfera de aplicación de las políticas de ciberseguridad para prevenir un conflicto o amenaza que puede afectar a la seguridad nacional de los Estados. Para enfrentar dichas amenazas las agencias de inteligencia juegan un papel fundamental recabando información para prevenir ataques.

1.2.5 Actividades de Inteligencia

Al hablar de seguridad nacional de un Estado, especialmente de los Estados Unidos, nos estamos refiriendo a las actividades de inteligencia, para intentar controlar las amenazas tanto internas como externas. También son actividades destinadas a obtener información que evite situaciones de vulnerabilidad del mismo. "La seguridad nacional, o la inseguridad nacional, es una ansiedad que aflige a los Estados de todo el espectro político: gobiernos de todo tipo han recurrido a los servicios de inteligencia para establecer una vigilancia político-

[39]Cita textual en ingles: *"Cyberspace: a global domain within the information environment consisting of the interdependent network of information technology infrastructures, and includes the internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries".* s/a, *Information and Cyberspace Issue Paper No. 1: information as an Element to Combat Power*, Department of Defense, Estados Unidos 21 febrero 2008, p. 6, Dirección URL: http://www.defense.gov/Blog_files/Blog_assets/20080408_ColParks_issuepaper.pdf, [Consultado el 27 de noviembre 2013].

policial nacional y, en un momento u otro, también han empleado el secreto o la policía política para reprimir lo que consideran un riesgo"[40].

Alberto Mendes considera que las actividades de inteligencia son "el ejercicio permanente de acciones para la obtención, evaluación, integración e interpretación de conocimientos del interés del Estado, […] Su función es vital cuando son utilizados en la operación de escenarios"[41].

Esta definición se complementa con lo que plantea Francisco Jijón, quien añade que esta inteligencia involucra la recolección e interpretación de información para proteger la seguridad del Estado y por tal razón "las actividades de Inteligencia conforman un proceso integrado de producción de conocimientos relativos a la seguridad interna y externa. Este conjunto lo constituyen labores inscritas dentro de las tareas institucionales desarrolladas en función de preservar la seguridad de los ciudadanos, habitantes y gobernantes, a través del goce pleno de sus libertades y derechos constitucionales y de la vigencia integral de las instituciones del régimen político legítimamente constituido"[42].

El procesamiento de esta información es de vital importancia para que los tomadores de decisiones tengan un mayor conocimiento y puedan anticipar información de ayuda para proyectar hacia el futuro algún fenómeno. Generalmente es utilizada para temas de seguridad y relaciones internacionales, pero existen otras esferas de acción como son la geoeconomía, la prevención de riesgos y la científico-tecnológica[43]. Por lo tanto, las actividades de inteligencia

---

[40] Whitaker Red, *El fin de la privacidad. Cómo la vigilancia total se está convirtiendo en realidad*, España, Ed. Paidós, 1999, p.32.
[41] Alberto Mendes Cardoso, *El papel de la actividad de inteligencia* en el inicio de una nueva era, en "Los servicios de inteligencia en el nuevo siglo", *Revista de Administración Pública*, Núm. 101, México, INAP, 2000, p. 25.
[42]Francisco Jijón Calderón, *Introducción: El Nuevo Ecuador y la Secretaría Nacional de Inteligencia* en Fredy Rivera Vélez, "Inteligencia estratégica y Prospectiva", Ed. FLACSO, Ecuador, mayo 2011, p. 17.
[43]Véase Jaime Castillo Arias, *Sistemas de Inteligencia. Perspectiva doctrinaria para realizar un análisis integral* en Fredy Rivera Vélez, "Inteligencia estratégica y Prospectiva", Ed. FLACSO, Ecuador, Mayo 2011, p. 83.

"proporcionan datos para enfrentar amenazas en la seguridad nacional y pública"[44], dado que la oportuna difusión de esta información brinda a los tomadores de decisiones la oportunidad de adoptar disposiciones para evitar que ocurran acciones y situaciones perjudiciales.

Estos servicios de inteligencia además de ser de utilidad para prevenir posibles amenazas o riesgos para el Estado, también son de gran utilidad para evidenciar ventanas de oportunidad que puedan ser de utilidad para el interés tanto actual como futuro de los países.

Las actividades de inteligencia consiste en: planificación, donde se establecen estrategias y mecanismos para acceder a la información; recolección de información de fuentes; elaboración: donde se transforma la información a través del análisis; conocimiento: esta información se entrega a los tomadores de decisiones y difusión de la información[45].

Durante la Segunda Guerra Mundial y la Guerra Fría las acciones de inteligencia fueron vitales para el desarrollo de la guerra. No obstante, tras el fin de la Guerra Fría se esperaba que estas se redujeran al haber vencido al enemigo soviético, cosa que no sucedió debido a que "los servicios de inteligencia, es decir, la adquisición intencional de información secreta, han sido un instrumento importante del poder estatal tanto en tiempos de guerra como de paz"[46]. Esto nos demuestra que estas no responden solamente a situaciones de conflicto bélico sino a momentos de estabilidad y si bien en los momentos de paz estas actividades disminuyen, nunca desaparecen por completo.

Tras el término de la Guerra Fría los servicios de inteligencia se trasformaron de "una combinación de actividades de inteligencia tradicionales, espionaje

---

[44]Ana María Salazar, *Seguridad Nacional Hoy. El reto de las democracias*, Ed. Nuevo Siglo Aguilar, México, 2002, p.114.
[45]Véase Central Intelligence Agency, 1993, Pp. 402-404.
[46]Red Whitaker, o*p. cit.*, p.10.

económico, guerra informática, proliferación y crimen transnacional"[47], debido a que las amenazas no desaparecen sino que evolucionan conforme se va trasformando la nueva realidad internacional.

Estas actividades si bien cuentan con un amplio respaldo al interior de los Estados Unidos como un elemento de defensa nacional, hacia el exterior han sido motivo de polémica, particularmente porque anteponen la defensa de su Estado frente a los otros.

1.2.6 Agencias de Inteligencia

Para definir a las agencias de inteligencia es preciso entender primero que se refieren a la información relevante para que los gobernantes y los tomadores de decisiones instrumenten políticas que consideren de interés de seguridad nacional y para hacer frente a las amenazas a estos intereses por parte de adversarios reales o potenciales[48]. También encontramos otra definición dada por Jeffrey Richelson quien plantea que la inteligencia es el producto resultante de la recolección, evaluación, análisis, integración e interpretación de información disponible, que es inmediata o potencialmente preocupante para algún aspecto del

---

[47] Pitfield D. Elcock Ward, *Perspectiva general de seguridad pública y seguridad nacional*, en "Los servicios de inteligencia en el nuevo siglo", *Revista de Administración Pública*, Núm. 101, México, INAP, 2000, p. 9.

[48]Cita textual en ingles: *"'Intelligence refers to 'information relevant to a government's formulation and implementing policy to further its national security interest and to deal with threats to those interests from actual or potential adversaries".* Shulsky, 2002, p.1 en Hans Born y Marina Caparini, Democratic Control of Intelligence Service: Containing Rogue Elephants, Gran Bretaña, Ed. Ashgate Publishing Company, 2007, p. 4, [en línea], Dirección URL: http://books.google.com.mx/books?id=FeGhAgAAQBAJ&pg=PA18&lpg=PA18&dq=intelligence+agencies+out+of+control&source=bl&ots=_jOMsbAOiX&sig=7ofbt8IGXVlXx1_BmrC1e8YVzU8&hl=es&sa=X&ei=lUUGVIWME4y-ggSWtICwCg&ved=0CFQQ6AEwBDgK#v=onepage&q=intelligence%20agencies%20out%20of%20control&f=false, [Consultado el 20 de febrero 2014].

exterior o de las áreas de operación[49]. Con estas dos definiciones podemos entender que la función de las agencias de las agencias de inteligencia es recabar, evaluar y analizar información que sea de utilidad para los tomadores de decisiones y ayude a prevenir amenazas latentes a la seguridad de los Estados.

Estas instituciones de inteligencia se crearon como un medio para que los Estados mantuvieran una vigilancia de la sociedad, la seguridad nacional y estabilidad del país. Es importante destacar que actualmente estas han utilizado los medios digitales como una de las principales vías para vigilar a la sociedad tanto nacional como internacional, principalmente a través de los medios cibernéticos como puede ser el correo electrónico, los celulares y el uso de Internet[50].

Analizar a las agencia de inteligencia es un problema complejo porque es necesario tomar en cuenta los alcances de las legislaciones en materia de seguridad cibernética, el papel de los directivos, la manera en la que estas organizaciones procesan la información y los vínculos que mantienen con organizaciones privadas, las cuales actualmente también analizan y evalúan información reservada.

Otro problema es que estas son realizadas por diferentes actores de las estructurales gubernamentales, con intereses y visiones diferentes, lo cual influye en el manejo de la información. Adicionalmente, "cada cambio directivo en el plano

---

[49]Cita textual en ingles: *"the product resulting from the collection, evaluation, analysis, integration and interpretation of all available information wich concerns one or more aspects of foreign nations or areas of operation which is immediately or potentially significant for planning".* Jeffrey Richelson en James J. F. Forest, Countering Terrorism and insurgency in the 21st Century, Estados Unidos, Ed. Praeger Security International,2007, p. 421, [en línea], Dirección URL: http://books.google.com.mx/books?id=RMUVEw1nfSUC&pg=PA421&dq=intelligence+agencies+definition&hl=es&sa=X&ei=B8EHVMXiB43IggSjsIKIBA&ved=0CCQQ6AEwAQ#v=onepage&q=intelligence%20agencies%20definition&f=false, [Consultado el 10 de agosto 2014].

[50]Véase s/a, *Supremo de EU rechaza revisar programas de espionaje*, [en línea], México, El Universal, 18 noviembre 2013, Dirección URL:http://www.eluniversal.com.mx/el-mundo/2013/espionaje-eu-snowden-966426.html, [Consultado el 3 de diciembre 2013] y Notimex, *Revelan espionaje de EUA y Reino Unido a Italia*, [en línea], México, El Universal 24 de octubre 2013, Dirección URL:http://www.eluniversal.com.mx/el-mundo/2013/espionaje-eu-italia-960534.html [Consultado el 3 de diciembre 2013].

político implica iniciar una nueva relación de confianza con la autoridad elegida, interacción que puede verse dificultada frente a la precariedad o débil institucionalidad de los sistemas de Inteligencia que no logran dar respuesta a todos los requerimientos inmediatos del decisor"[51]. Por lo cual problemas o conflictos internos pueden ocasionar que estas agencias no cumplan con su cometido, se dé un manejo inadecuado de esta información o no resguarden adecuadamente los datos que están manejando.

1.2.6.1 Espionaje y ciberespionaje

El espionaje es una práctica histórica de los gobiernos, podríamos decir que ha existido desde siempre en la historia del hombre, como un medio para conocer alguna información sobre alguien más. Según el Glosario de Inteligencia de Miguel Ángel Esteban Navarro[52], un espía es <aquella persona que por encargo de alguien, sea un servicio de inteligencia o no, se dedica a obtener información de un tercero, de manera clandestina, con engaño y sin autorización de este último>.

A pesar de que ha sido una práctica común no fue sino hasta el siglo XX que las actividades de espionaje adquieren un carácter institucional, organizado y sistemático debido al importante papel que adquieren las agencias de inteligencia durante la Segunda Guerra Mundial y la Guerra Fría.

A pesar que el auge del espionaje se dio durante la Guerra Fría, esta actividad coexiste hasta la actualidad en razón de que "[…] la inseguridad internacional provoca generalmente miedo respecto a la seguridad nacional y el enemigo interior, ya que las patologías del contraespionaje (…) están íntimamente

---

[51]Fredy Rivera Vélez y Katalina Barreiro Santana, *Inteligencia estratégica: algo más que curiosidad mediática o (in) discrecionalidad política*, en Fredy Rivera Vélez, Inteligencia estratégica y Prospectiva, Ecuador, Ed. FLACSO, Mayo 2011, p. 33.

[52]Véase Miguel Ángel Esteban Navarro Coordinador, "Glosario de Inteligencia" Ministerio de Defensa de España, España 2007 en Juan Carlos Herrera Hermosilla, *Breve Historia del Espionaje,* España, Ediciones Nowtilus, 2012, p.14.

vinculadas a la percepción del enemigo interior en tanto que una insidiosa extensión del enemigo exterior"[53].

Los Estados realizan espionaje para obtener información de los demás. Sin embargo, a su vez el resto de los gobierno realizan actividades de espionaje para impedir que los primeros obtengan información de ellos a lo que se denomina contraespionaje o contrainteligencia, el cual consiste en una "serie de métodos utilizados para obtener información que permita impedir que un adversario obtenga datos que pudieran dar una ventaja"[54]. Esto genera que los Estados estén en constante alerta frente a los demás, volviéndose un círculo de inseguridad internacional donde **"**se espían entre ellos y tratan de protegerse del espionaje de sus rivales, razón por la cual nació el Estado de inseguridad nacional, con sus informes secretos y con sus bancos de datos que almacenan las creencias y las ideologías políticas de sus ciudadanos"[55].

Es necesario entender que esta búsqueda de la seguridad nacional ha llevado a los Estados a:

> "[…] establecer y reforzar la policía secreta y los servicios nacionales de inteligencia, a pesar del impedimento que pudiesen suponer las constricciones nacionales y los derechos humanos; al intentar controlar, o por lo menos gestionar, información de interés de la seguridad del Estado; y al movilizar el saber en interés del poder"[56].

Punto fundamental para esta investigación ya que con base en este principio, el gobierno norteamericano ha establecido políticas de vigilancia mundial que la opinión pública ha llegado a considerar como violaciones a la soberanía nacional y a los derechos humanos, de los que hablaremos más adelante.

---

[53] Red Whitaker, *op.cit.,* p.33.
[54] Shulsky, 1995, pp.4 en Ana María Salazar, Seguridad Nacional Hoy. El reto de las democracias, Ed. Nuevo Siglo Aguilar, México, 2002, p. 117.
[55] Red Whitaker, *op.cit.,* p.39.
[56] *Ibid.*, p.44.

Por otra parte, existe otra forma de espionaje dentro del ciberespacio que ha adquirido mayor relevancia gracias a los nuevos avances tecnológicos que han facilitado la obtención de información de manera más rápida, eficaz y sin necesidad de ser percibidos. Lo que ha llevado a que los individuos pierdan su privacidad, gracias a que dentro del ciberespacio "el individuo tiende a convertirse en un registro más de la gigantesca base de datos, manipulada tanto por los organismos del Estado, como por innumerables empresas"[57]. Gracias a esto el ciberespionaje se ha convertido en una amenaza latente para el mundo, ya que la pérdida de información confidencial a través de trasferencias electrónicas puede generar desastres económicos, diplomáticos y políticos, por lo que los países han incrementado este tipo de actividades para adquirir información clasificada de otros gobiernos y para preservar los intereses nacionales de las empresas para tener ventajas frente a ellas en posibles negociaciones.

1.2.7 Wikileaks

En particular para esta investigación nuestro objeto de estudio, es el caso de Wikileaks. Según su portal de Internet[58], Wikileaks es una organización de medios sin fines de lucro, que funciona de manera independiente, que incluye dentro de su equipo a periodistas, programadores de software, ingenieros, matemáticos, etc. Para Enrique Dans "Wikileaks es un gestor de información. En su funcionamiento Wikileaks intenta reducir en la medida de lo posible las barreras de entrada al llamada *whistelblowing*, al filtrado de información"[59], razón por la cual esta organización tiene por objetivo brindar información y noticias al púbico, de una manera innovadora, segura y anónima para las fuentes que le brinden

[57]Alberto Romero, *Globalización y pobreza*, Ed. Universidad de Nariño, Colombia, marzo 2002, p.70.
[58] Véase About Wikileaks, [en línea] Dirección URL: http://wikileaks.org/About.html, [Consultado el 10 de diciembre 2013].
[59] Julian Assange; Jacob Appelbaum; Andy Muller-Maguhn y Jérémie Zimmermann, *Cypherpunks: La Libertad y el futuro del Internet*, España, Ed.Grupo Planeta, 2013, p.12.

información. Su principal actividad es publicar material original para que los lectores puedan tener evidencia de lo que en realidad está pasando.

Esta organización se creó en 2006 por Julian Assange[60] como fundador, la cual ha logrado permanecer abierta a pesar de los ataques legales y políticos para intentar silenciar la organización. Los principios fundamentales de este grupo son la defensa de la libertad de expresión y los medios, apoyo de los derechos de todas las personas para crear historias y mejorar el registro histórico común, que está estipulado en el artículo 19 de la Declaración Universal de los Derechos Humanos.

Wikileaks funciona mediante el periodismo de investigación, aceptando fuentes anónimas por medio de un buzón de anónimo para proteger a sus fuentes. Esta organización argumenta que busca conseguir la verdad. Con base en este principio ético se analiza y verifica la veracidad de la información, para posteriormente publicar la noticia. Se publica el material original, para que los lectores puedan analizar la información dentro del contexto original.

Esta organización considera importante publicar la información a la que tiene acceso por considerar que es un medio para mejorar la trasparencia y de esta manera beneficiar a la sociedad. Se argumenta también que al dar a conocer esta información se logrará romper con las redes de corrupción, exponer los engaños por parte del gobierno y las clases dominantes. Asimismo, se considera una organización a favor de la libertad de expresión y los medios de comunicación, por

---

[60] Julian Assange periodista, hacker, activista y programador australiano, estudió física y matemáticas en la Universidad de Melbourne. Ha recibido varios premios y condecoraciones por sus trabajos de periodismo y libertad de expresión como el Premio Amnistía Internacional de los Medios Británicos en 2009. Actualmente se encuentra refugiado bajo asilo diplomático en la Embajada de Ecuador en Londres para refugiarse de una extradición a Suecia por los delitos de violación y acoso sexual a dos jóvenes en este país de los que se le acusa. Adicionalmente, el gobierno de los Estados Unidos inició una investigación criminal sobre Julian Assange con apoyo del Departamento de Justicia y el FBI, para analizar si se les puede imputar cargos bajo la Ley de Espionaje de 1917. Está a la espera de un salvoconducto del gobierno de Reino Unido que le permita salir es este país y solicitar asilo en Ecuador.

no tener un vínculo con el gobierno, porque considera que supera a los tradicionales medios de comunicación, que no eran independientes y respondían ante los grupos dominantes.

Desde la perspectiva de Wikileaks, generó un nuevo modelo de periodismo en el mundo, ya que por una parte es una organización que no está motivada directamente por una ganancia, que establece lazos de cooperación con otros medios de comunicación, para romper de esta manera con el esquema periodístico tradicional de competencia por la información. Además de que parte del principio de no acumular la información para el momento oportuno, sino dar a conocerla en el momento que la reciben[61].

La información presentada por Wikileaks es verificada a través de un análisis forense del documento: se determina el costo de falsificación, medios, motivos, la oportunidad, preguntas detalladas sobre el contenido, al igual que se puede recurrir a una verificación externa de la información lo cual consiste en enviar un equipo de periodistas a entrevistas a personas afectadas u observadores de ser posible, al igual que buscar otras pruebas que corroboren la verdad de la historia, sin embargo, aceptan que puede haber errores en este proceso aunque hasta el momento, no se han dado casos[62].

En el prólogo de la versión en español del libro Cypherpunks: La libertad y el futuro de internet, Enrique Dans, considera que "Wikileaks es el signo de los tiempos: el desarrollo y popularización de la red como herramienta en manos de una parte significativamente mayoritaria de las sociedades desarrolladas ha

[61]s/a, Why the media (and particularly Wiki leaks) is important, Wikileak.org, Dirección URL: https://wikileaks.org/About.html, [Consultado el 14 de diciembre 2013].
[62] s/a, About Wikileaks, Dirección URL:https://wikileaks.org/About.html, [Consultado el 14 de diciembre 2013].

determinado que muchas de las cosas que antes tenían lugar en secreto, dejen de transcurrir en la oscuridad"[63].

A pesar de que de que esta organización se considera un nuevo medio de comunicación, algunos ex funcionarios del gobierno como Abbe. D Lowell[64] y Paul Rosenzweig[65] consideran que las organizaciones periodísticas se enorgullecen de brindar mayor valor a las noticias analizado y contextualizando la información, y el caso de Wikileaks simplemente funge como un compilador de información, que no discrimina los datos que proporciona[66], por lo que no debe ser considerado como un nuevo medio de comunicación. Por otra parte, Hillary Clinton mencionó que Wikileaks ataca los intereses nacionales en el exterior de los Estados Unidos y de la comunidad internacional[67].

Sin embargo, existe otra postura predominante entre los periodistas, quienes se encuentran a favor de Wikileaks y están agradecidos por los éxitos que ha logrado esta organización, la importancia que tiene este fenómeno para el periodismo y la trasparencia, que se puede observar claramente en lo que plantea Jason Deans, haciendo referencia a que Wikileaks es el portador de un nuevo fenómeno de la era digital. Es más, debido a su meta de justicia a través de la trasparencia sigue

---

[63] Julian Assange, Jacob Appelbaum; Andy Muller-Maguhn y Jérémie Zimmermann, *Cypherpunks: La Libertad y el futuro del Internet*, o*p.cit.,* p.10

[64] Socio abogado de la firma McDermott Will &Emery.

[65]Ex funcionario del Departamento de Seguridad Nacional durante la presidencia de George W. Bush como subsecretario adjunto para política y secretario adjunto para asuntos internacionales. Actualmente es investigador visitante en el Centro de Estudios Legales y Judiciales de la Escuela de la Universidad George Washington.

[66]Cita textual en ingles: "*New organizations pride themselves on adding value to news- they analyze and provide context. Wikileaks does none of that. It's more like a telephone directory- just a compiler of information, not a discriminating purveyor-".* Bill Dedman, U.S. v. WikiLeaks: espionaje and the First Amendment, NBC News, Dirección URL:http://www.nbcnews.com/id/40653249/#.UowdEtJFWSo, [Consultado el 19 de noviembre de 2013].

[67]Cita textual en ingles: "*Wikileaks' release an "attack on America's foreign policy interests" and on the international community*" .Ujala Sehgal, *Hilary Clinton: WikiLeaks Is An "Attack On America's Foreign Policy Interests,* 29 de noviembre, *Dirección URL* http://www.businessinsider.com/hilary-clinton-on-stolen-documents-2010-11#ixzz2lDXVY29C, [Consultada el 15 de diciembre 2013].

los estándares tradicionales periodísticos más antiguos[68]. Resumiendo, hay quienes se encuentran a favor y consideran que Wikileaks es una organización novedosa, que intenta mejorar la libertad de expresión y la trasparencia. Y los que la desaprueban, considerando que no puede ser una organización periodística, porque no realiza un análisis y contextualización de la información que difunde.

1.2.8 *Cablegates*

Se conoce como *Cablegates* o también como *United States diplomatic cable leak*, o *Secret US Embassy Cables*, a la filtración por Wikileaks a la prensa internacional el 28 de noviembre de 2010, de 251,187 cables del Departamento de Estado de los Estados Unidos sobre comunicaciones con sus embajadas en el mundo. Gracias a su exorbitante número, se convirtió en la filtración de documentos confidenciales más grande para el dominio público, que fueron proporcionados a algunos de los principales periódicos del mundo, como *The Guardian* diario británico, *The New York Times* diario norteamericano, *Le Monde* diario francés, El País diario español y *Spiegel* semanario alemán.

Dentro de estos cables se encuentran comunicaciones de la Administración central estadounidense hacia sus diplomáticos y viceversa, comunicaciones entre las diferentes embajadas de los Estados Unidos que abarcan un periodo de diciembre de 1966 hasta febrero de 2010, aunque se centran principalmente en los años 2008 y 2009.

---

[68]Cita textual en ingles: "*WikiLeaks has been portrayed as a phenomenon of the hi-tech age, which it is. But it's much more. Its goal of justice through transparency is in the oldest and finest tradition of journalism. WikiLeaks has given the public more scoops than most journalists can imagine: a truth-telling that has empowered people all over the world. As publisher and editor, Julian Assange represents that which journalists once prided themselves in –he's brave, determined, independent: a true agent of people not of power (quoted in Deans, 2011).* Jason Deans, "Julian Assange wins Martha Gellhorn journalism prize." [en linea], *The Guardian, 2 de junio 2011, Dirección URL:* http://www.theguardian.com/media/2011/jun/02/julian-assange-martha-gelhorn-prize, [Consultada el 15 de diciembre 2013].

En estas se revelan detalles de campañas bélicas, conflictos diplomáticos y evidencia de cómo funcionan las 274 embajadas estadounidenses en todo el mundo, haciendo referencia a muchos países dentro de ellos a Afganistán, Alemania, Arabia Saudita, Argentina, Australia, Bolivia, Bosnia Herzegovina, Brasil, Canadá, Chile, China, Colombia, Corea del Norte, Corea del Sur, Cuba, Ecuador, Egipto, El Salvador, Emiratos Árabes Unidos, España, Francia, India, Irán, Israel, Italia, Japón, Kosovo, Kuwait, México, Nicaragua, Pakistán, Panamá, Paraguay, Perú, Reino Unido, Rusia, Serbia, Siria, Sudáfrica, Turquía, Uruguay, Venezuela y Yemen.

Esta información fue filtrada a través del sistema de Internet de Ejército norteamericano: *Secret Internet Protocol Router Network* (SIPRNET, siglas en ingles), que es el sistema que utilizaban las 180 embajadas norteamericanas en el mundo. Que si bien si cuenta con fuertes medidas de seguridad para su uso como "mantenerlo abierto únicamente cuando el usuario está frente a la pantalla, exigencia de cambiar la clave cada cinco meses o la prohibición de utilizar CD u otros discos extraíbles para copiar contenidos, el número de personas que acceden a la información ha crecido".[69] A pesar de estas medidas de seguridad fue posible para Bradley E. Manning un soldado de 22 años de primera clase, analista de inteligencia categoría 35F, el utilizar su puesto en una base militar en Bagdad para obtener los documentos del Departamento de Estado los cuales fueron copiados dentro de un CD de música sin ser descubierto.

De los 251,187 cables filtrados 15,652 están clasificados como "secreto", 9,000 están identificados como "*NOFORN*" que es la abreviación para demasiado delicado para ser compartido con ningún gobierno extranjero, 4000 están designados como "*SECRET* y *NOFORN*", y 101,748 están clasificados como

[69] Véase. Preguntas y respuestas sobre los papeles del Departamento de Estado, El País, Madrid, 28 de noviembre de 2010, Dirección URL: http://internacional.elpais.com/internacional/2010/11/28/actualidad/1290898811_850215.html, [Consultado el 22 de octubre de 2013].

confidenciales, mientras que el resto de los informes, es decir 133,887, se encuentran en la categoría de no clasificado y ninguno de ellos está marcado como *"Top Secret"*[70].

Algunos de los cables contienen descripciones brindadas por los diplomáticos sobre corrupción por parte de los regímenes extranjeros, información sobre envío de armas clandestinas, trata de personas, violaciones a derechos humanos y los esfuerzos por sancionar a los países que cuentan con armas nucleares como Irán y Libia. Sin embargo, no se tiene acceso a documentos más secretos o "*Top Secret*" debido a que estos documentos no se encontraban dentro del sistema electrónico SIPRNET.

Los temas más frecuentes de estos cables según la clasificación del Departamento de Estado de los Estados Unidos son: relaciones políticas exteriores, con 145,451 cables, asuntos gubernamentales internos 122,896 cables, derechos humanos 55,211 cables, condiciones económicas 49,044 documentos, sobre terroristas y terrorismo 28,801 documentos y finalmente del Consejo de Seguridad de las Nacionales Unidas se revelaron 6,532 documentos.

El gobierno de los Estados Unidos consideró que "estas revelaciones ponen en riesgo a nuestros diplomáticos, profesionales de inteligencia y personas de todo el mundo que vienen a Estados Unidos para ayudar en la promoción de la democracia y de un gobierno abierto"[71] en palabras de Hilary Clinton, lo cual significó un importante golpe diplomático y de legitimidad que más adelante analizaremos.

---

[70] Scott Shane y Andrew W. Lehren, "Leaked Cables Offer Raw Look at U.S. Diplomacy", [en línea], *The New York Times*, 28 de noviembre 2010, Dirección URL: http://www.nytimes.com/2010/11/29/world/29cables.html?pagewanted=1&_r=0&hp, [Consultado el 25 de octubre de 2013].

[71]Redacción BBC Mundo, *Wikileaks: EE.UU. trata de contener el daño diplomático*, [en línea], BBC Mundo, 29 de noviembre 2010, Dirección URL: http://www.bbc.co.uk/mundo/noticias/2010/11/101128_wikileaks_documentos_eeuu_cables_preocupaciones_chavez_amab.shtml?print=1, [Consultado el 2 de diciembre de 2013].

Capítulo 2 Políticas de seguridad informática en los mandatos presidenciales de los Estados Unidos (2001-2013)

Los atentados terroristas en contra de los Estados Unidos de América el 11 de septiembre de 2001, modificaron la concepción de seguridad nacional del gobierno norteamericano en todos los ámbitos. Un área que cambió radicalmente fue la ciberseguridad, donde el gobierno instrumentó diversas medidas y estrategias que fueron evolucionando con las distintas administraciones gubernamentales. Aunado a ello, aparecieron nuevas amenazas a la par de un acelerado desarrollo tecnológico, que hizo evidente algunas vulnerabilidades en los programas cibernéticos y, por consecuencia, implicó una debilidad para el gobierno que quedó expuesto a posibles ataques en su contra.

Esta dinámica puso de manifiesto la importancia de asegurar la infraestructura crítica para evitar un ataque cibernético, ya que un ataque de esta naturaleza a las redes gubernamentales traería graves consecuencias en distintos niveles, como veremos más adelante, con la filtración de información por parte de Wikileaks, como explica de manera clara John Rolling, quien considera que el incremento de amenazas cibernéticas y a la infraestructura de telecomunicaciones del gobierno de los Estados Unidos, se puede explicar debido al incremento de la capacidad para dañar a este país en materia de seguridad cibernética[72].

Por tal razón se establecieron políticas de seguridad cibernética para asegurar la seguridad nacional en el ciberespacio. Estos recursos pueden ser tanto tecnológicos como estructurales (programas y estrategias, organizacionales), así como de recursos humanos (capacitación de personal).

---

[72]Cita textual en ingles**:** *"threats to the U.S cyber and telecommunications infrastructure are constantly increasing and evolving as are the entities that show interest in using a cyber-based capability to harm the nation's security interests"* John Rollins y Anna C. Henning, Comprehensive National Cybersecurity Initiative: Legal Authorities and Policy Considerations, Congressional Research Service, 10 de marzo 2009, p. 2.

Por tal razón, es fundamental para esta investigación analizar las posturas en materia de seguridad cibernética de las últimas dos administraciones de los Estados Unidos, con la finalidad de conocer su evolución, así como sus alcances y limitaciones.

2.1 La administración de George W. Bush (2001- 2009)

La estrategia de George W. Bush[73] para enfrentar el terrorismo fue holística porque no sólo modificó aspectos militares y legales, sino que también incorporó a la seguridad cibernética como una prioridad, al reconocer que existían vulnerabilidades en las redes gubernamentales. Esta administración puso en marcha políticas claras y concretas en materia de seguridad cibernética, que se convirtieron en el marco de referencia para regular la seguridad cibernética de los Estados Unidos, partiendo de la necesidad de conjuntar al sector privado y al público para lograr proteger la infraestructura crítica.

Tras los atentados terroristas del 11 de septiembre de 2001 el entonces Secretario de Defensa, Donald Rumsfeld, estableció una serie de acciones para disuadir a los posibles enemigos, las cuales consistían en combatir a las redes terroristas y a todos los que las apoyaran utilizando todas las herramientas necesarias en su

[73]George W. Bush nació el 6 de julio de 1946 en New Haven Connecticut. Asumió el cargo de la presidencia el 20 de enero de 2001, convirtiéndose en el presidente número 43 de los Estados Unidos. Su mandato presidencial se caracterizó por el endurecimiento de políticas contra el terrorismo. Fue reelecto para un segundo periodo el 20 de enero de 2005. Anteriormente fue gobernador de Texas y participó en la campaña presidencial de su padre George Bush. Licenciado en historia por la Universidad de Yale en 1986, maestría en administración de empresas por de Harvard Business School en 1975. Véase: Presidentes de los Estados Unidos, [en línea], White House, Dirección URL:http://georgewbush-whitehouse.archives.gov/president/gwbbio.es.html, [Consultado el 16 de diciembre 2013].

poder ya fueran diplomáticas, económicas, financieras, de inteligencia y militares, entre otras[74].

Por lo tanto era necesario el establecer reglas para normar actividades que podrían favorecer las actividades terroristas como lo fue la creación de la Acta Patriótica de la que hablaremos más adelante, la cual establece políticas para:

> "[…] innovar las fuerzas armadas (…) a través de la experimentación con nuevas concepciones militares, el reforzamiento de las operaciones conjuntas, el aprovechamiento de las ventajas del sistema de inteligencia americano y sacar el máximo provecho a la ciencia y la tecnología"[75].

La estrategia de seguridad nacional que adoptó el Departamento de Defensa consistía en:

> "[…] primero proteger el territorio estadounidense y nuestras bases en el exterior; segundo, enviar fuerzas a escenarios distantes y mantenerlas allí; tercero, impedir que nuestros enemigos encuentren refugio asegurándonos que sepan que ningún rincón del mundo… será suficientemente remoto… para huir de nuestro alcance; cuarto, proteger nuestras redes de información; quinto, utilizar la tecnología de información para entrelazar los distintos tipos de fuerza de los EE.UU.; sexto, mantener sin trabas el acceso al espacio y proteger de cualquier ataque nuestros recursos en el espacio"[76].

Ello llevó al gobierno de los Estados Unidos a adquirir un papel de liderazgo a nivel internacional, con el fin de crear un ciberespacio seguro y establecer leyes

---

[74]Cita textual en inglés: "*We must fight terrorist networks and all those who support their efforts to spread fear around the world using every instrument of national power- diplomatic, economic, law enforcement, financial, information, intelligence, and military".* White House, National Strategy for Combation Terrorism. Washington, DC. Government Printing Office, Feb 2003 en Baylis John, Wirtz Jamens, Gray Colin S. y Cohen Eliot, *Strategy in the contemporary World*, Estados Unidos, Ed. Oxford University Press, 2007, p.203.

[75] George W. Bush, "La estrategia de seguridad nacional de los Estados Unidos de América", *Revista Internacional de Filosofía Política*, México, Ed. UAM Iztapalapa, Julio 2003, No. 21, p. 232.

[76] Fuentes Claudio, *Bajo la mirada del halcón: Estados Unidos-América Latina post 11/9/2001*, Chile, Ed. Biblos, FLACSO, 2004, p. 35.

internacionales para resguardarlo. Se parte del supuesto de que los Estados tienen la obligación de resguardar el ciberespacio y por tal razón es indispensable que cooperen para evitar atentados[77].

Es decir, se parte del supuesto de que los demás Estados se responsabilizarán de las acciones que realizan sus ciudadanos dentro del ciberespacio, ya que el control individual de Estados Unidos resultaba insuficiente para enfrentar las posibles amenazas en el ciberespacio y por tanto requería de la cooperación y coordinación de otros estados.

Asimismo, los atentados terrorista de 2001 hicieron evidentes fallas en los servicios de inteligencia de los Estados Unidos, por lo cual la administración de George W. Bush creó un nuevo modelo que permitiera establecer comunicación entre los diferentes responsables de la seguridad nacional estadounidense y brindar la posibilidad de compartir datos del Departamento de Estado a través del *Secret Internet Protocol Router Network* (SIPRNET, siglas en ingles)[78].

La administración de George W. Bush incrementó su Estrategia de Seguridad, en varios campos: estableció responsabilidades sobre la seguridad territorial (incluyendo la ciberdefensa); creó una legislación para Seguridad Nacional y ciberdefensa; estableció planes y estrategias de seguridad nacional en distintos niveles: seguridad territorial, seguridad cibernética, ejercicios periódicos de

---

[77] Cita textual en ingles: *"A central part of that effort is to get all nations to agree that international law applies to cyberspace, that states have the same responsibilities in cyberspace as they do in other areas, and that nations should cooperate in security and law enforcement".* James Andrew Lewis, Private Retaliation in Cyberspace, [en línea], CSIS, 22 de mayo 2013, Dirección URL :https://csis.org/publication/private-retaliation-cyberspace, [Consultado el 19 de diciembre de 2013].

[78] SIPRNET sustituyó a DDN DSNET1, es un sistema de redes de computadora conectadas, que funciona como una versión secreta de Internet utilizado por el Departamento de Defensa y el Departamento de Estado de los Estados Unidos para transmitir información clasificada (incluyendo información clasificada como SECRET) por conmutación a través de protocolos TCP (Protocolo de Control de Transmisión es la base de Internet con diferentes sistemas operativos), que proporciona también servicios de documentos de hipertexto y correo electrónico. Véase Secret Internet Protocol Router Network (SIPRNET), [en línea], US MIlitary, Dirección URL: http://www.usmilcom.com/military.htm, [Consultado el 20 de diciembre de 2013].

ciberseguridad, creó un Plan Nacional de Protección de Infraestructura y seminarios periódicos de concienciación sobre ciberseguridad[79].

Específicamente, en materia de ciberseguridad, la administración de George W. Bush estableció cinco prioridades tras los atentados:

1. La creación de un Sistema de Repuesta Nacional de la Seguridad en el Ciberespacio, surgiendo en 2003 el *United States-Computer Emergency Readlness Team* (US-CERT, siglas en ingles)[80], para analizar las amenazas cibernéticas y difundir alertas sobre posibles amenazas.
2. Reducción de amenazas y vulnerabilidad sobre Seguridad en el ciberespacio.
3. Formación y concientización de la ciberseguridad.
4. Asegurar el ciberespacio gubernamental.
5. Cooperación nacional e internacional[81].

En virtud de lo anterior podemos llegar a una primera conclusión sobre las políticas de seguridad cibernéticas de George W. Bush: que las estrategias giran en torno a dos prioridades, por una parte la lucha frontal contra el terrorismo y el enemigo externo y por la otra enfrentar la amenaza de infiltraciones a través de mecanismos tecnológicos frente a lo cual resulta insuficiente la intervención de las autoridades gubernamentales.

---

[79]Cyber Storm III en el cual se integran empleados de siete departamentos de gobierno, 60 empresas privadas y 12 socios internacionales, que son organizados por el Departamento de Seguridad Nacional (primer intento para crear un centro de seguridad cibernética en el gobierno de los Estados Unidos).

[80] US-CERT (siglas en ingles) es parte del Departamento de Seguridad Nacional de los Estados Unidos y funciona como la parte operativa en materia de ciberseguridad de éste Departamento. Se encarga de liderar los esfuerzos para mejorar la seguridad cibernética, a través del intercambio de información y gestionar los riesgos de manera proactiva. Véase: About US, [en línea], US-CERT, Dirección URL:http://www.us-cert.gov/about-us, [Consultado el 20 de diciembre de 2013].

[81] Javier Candau Romero, *Estrategias Nacionales de Ciberseguridad. Ciberterrorismo*, pp.275- 276. En Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio, [en línea], Ministerio de Defensa de España, Diciembre 2010http://bibliotecavirtualdefensa.es/BVMDefensa/i18n/catalogo_imagenes/grupo.cmd?path=17029, [Consultado el 23 de enero de 2014].

Para el establecimiento de las políticas en materia de seguridad cibernética, el gobierno de los Estados Unidos creó nuevas leyes y diseñó nuevas estrategias destinadas a fortalecer la seguridad del manejo de la información en el ciberespacio. A continuación hablaremos de algunas de las principales para posteriormente hacer un análisis de qué sus alcances en el mantenimiento de la seguridad cibernética.

2.1.1 Ley Patriota 2002

La Ley Patriota o también conocida como Unidad y Fortalecimiento de América creada para proporcionar medidas adecuadas para interceptar y obstruir al terrorismo, surgió a raíz de los atentados terroristas del 11 de septiembre de 2001. Entró en vigor el 26 de octubre de 2001 y fue aprobada por mayoría en ambas cámaras del Congreso de los Estados Unidos. Su principal propósito era fortalecer la seguridad doméstica de los Estados Unidos siguiendo la visión estratégica del gobierno de George W. Bush, de que la lucha contra el terrorismo era la prioridad nacional. Consistía en concentrar los esfuerzos en cuatro principios: derrotar, negar, discriminar y defender, incorporando un ataque integral en contra de la organización terrorista. Atacando no solamente a las redes en sino también sus liderazgos y financiamitos[82].

Esta Ley se convirtió en la base legal dentro de la legislación norteamericana para combatir al interior cualquier acto terrorista, razón por la cual abarca diversos temas sobre la seguridad de los Estados Unidos tales como mejorar los servicios de seguridad nacional; la prevención contra el lavado de dinero como medio para evitar su financiamiento; el endurecimiento de políticas de seguridad fronteriza; la eliminación de obstáculos para la investigación de actividades terroristas y la protección a víctimas de terrorismo.

---

[82] Cita textual en ingles**:** “encapsulated in 4 Ds- defeat, deny, diminish, and defend- incorporated a comprehensive attack on terrorist organization through targeting not only the networks themselves but also their leadership, sanctuaties, and finances” John Baylis, Jamens Wirtz, Colin S. Gray *et.al Strategy in the contemporary World,* Estados Unidos, Ed. Oxford University Press, 2007, p.203.

Para esta investigación nos enfocaremos en el Título II de la Ley Patriota referente a los Procedimientos de Vigilancia Mejorada, la cual brinda mayores atribuciones a las agencias del gobierno para reunir información de inteligencia extranjera tanto de ciudadanos norteamericanos como de extranjeros, mediante el rastreo de comunicaciones, escuchas telefónicas incluyendo direccionamientos y enrutamientos y el uso de contraespionaje[83].

Esta ley da la posibilidad de que cualquier juez en cualquier tribunal de los Estados Unidos emita una orden de vigilancia de comunicaciones en todo el territorio estadounidense. Esto trae como consecuencia que las personas afectadas estén prácticamente imposibilitada para solicitar la revisión de la orden judicial emitida, siempre y cuando el FBI justifique el motivo de la petición de registro en pro de la seguridad, incluso si el investigado es ciudadano norteamericano[84]. De igual modo otorga mayores posibilidades a las agencias de inteligencia de tener acceso a correos de voz, a interceptar comunicaciones electrónicas y telefónicas, con lo cual se permitió eliminar una restricción legal en las investigaciones penales y de vigilancia.

Por otra parte, esta ley trajo consigo modificaciones a la *Foreign Intelligence Surveillance Act* (FISA, siglas en ingles), con lo cual se eliminó el requisito necesario para establecer la vigilancia de una persona extranjera, en la cual se hacía referencia a que el gobierno debía demostrar cuál era el objetivo de las investigaciones antes de realizar una vigilancia. Esta modificación generó controversia ante la opinión pública que consideraba que esta violaba los

---

[83]Uniting and Strengthening America by providing appropriate tools required to intercept and obstruct terrorism (USA Patriot Act) Act 2001, [en línea], 26 de octubre de 2001, Dirección URL:http://www.gpo.gov/fdsys/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf, [Consultado el 10 de enero 2014].

[84]Alan Graf, *Guerra y represión: la 'USA-Patriot Act' recorta los derechos civiles y ataca las libertades fundamentales en EEUU so pretexto de garantizar la "seguridad nacional",* [en línea], Avizora, 17 de mayo 2010, Dirección URL:http://www.avizora.com/atajo/informes/usa_textos/usa_textos_2/0037_ley_patriotica.htm, [Consultado el 15 de julio 2014].

derechos humanos, al permitir investigar a una persona de manera arbitraria sin una orden jurídica.

El Título IX de esta ley referente *a Mejorar la Inteligencia* también es relevante para esta investigación, ya que modifica la Ley de Seguridad Nacional de 1947[85], lo que permitió que la información recolectada por las agencias de inteligencia pudiera ser consultada por otras instituciones. El resolutivo fue criticado por considerar que "(…) Las modificaciones de la *Patriot Act* han reducido los requisitos a que "un importante propósito de la vigilancia sea obtener inteligencia extranjera"[86].

En consecuencia, el Gobierno puede evitar el protocolo que exige la Cuarta Enmienda, consistente en demostrar al juez que existe causa probable de la comisión de un delito y que intervienen para obtener pruebas[87]. Es decir, esta ley brinda mayor autoridad a los funcionarios federales para interceptar comunicaciones como una medida de vigilancia y contraespionaje frente al terrorismo. Sin embargo, estas atribuciones podrían atentar contra algunos derechos fundamentales de los ciudadanos, de ahí lo polémico.

En suma, la Ley Patriota es un documento relevante en materia de seguridad cibernética ya que vincula las tres preocupaciones de la administración de George W. Bush: la lucha contra el terrorismo, la seguridad nacional y la seguridad cibernética.

---

[85] Esta ley estableció la estructura de seguridad nacional que perdura hasta el día de hoy en los Estados Unidos post- Guerra Fría. Fusionó el Departamento de Guerra, y el Departamento de la Marina en el Establecimiento Militar Nacional (NME, siglas en ingles) encabezado por el Secretario de Defensa y creó el Departamento de la Fuerza Aérea.

[86] Sundby Scott E. y Pérez Cebadera María Ángeles, Caminando sobre la cuerda floja constitucional: la USA *Patriot Act* y la "Guerra contra el terror", [en línea], *Revista General de Derecho Procesal,* 2008, Dirección URL: http://repositori.uji.es/xmlui/bitstream/handle/10234/19013/29277.pdf?sequence=1, p. 8. [Consultado el 10 de enero 2014].

[87] *Ibidem.,* p. 8.

2.1.2 Ley Federal de Manejo de Seguridad Informática (FISMA)

La Ley Federal de Manejo de la Seguridad Informática (FISMA por sus siglas en inglés) fue promulgada en 2002 como el Título III de la Ley de Gobierno Electrónico de 2002. Se encuentra bajo la responsabilidad del Departamento de Seguridad Nacional y establece apoyo operativo a las agencias federales en el mantenimiento de la seguridad de los sistemas federales.

Tiene como principal propósito generar revisiones periódicas de los programas de seguridad informática de las diferentes dependencias gubernamentales que se utilizan para supervisar y elaborar un informe anual que se entrega al Congreso de los Estados Unidos, para que éste conozca los riesgos y tenga la posibilidad de responder rápidamente frente a una amenaza.

Brinda responsabilidades a los distintos organismos para garantizar la seguridad de los datos del gobierno de los Estados Unidos, el Instituto Nacional de Estándares y Tecnología (NIST, siglas en ingles)[88] es la institución encargada de establecer los protocolos básicos de seguridad informática. Es por ello que se crearon nueve pasos para garantizar la seguridad de la información que consisten en: categorizar la información; seleccionar controles mínimos; mejorar los controles a través de una evaluación de riesgos; documentar los controles en un plan de seguridad del sistema; instrumentar controles de seguridad; evaluar la efectividad de los mismos; determinar los riesgos; autorizar el sistema de información y la supervisión de los controles de seguridad[89].

La FISMA define tres objetivos que son indispensables para asegurar la información electrónica: el primero consiste en entender que la información debe

---

[88] Es el encargado de desarrollar normas, lineamientos y directrices para asegurar la información de las agencias a través de FISMA. National Institute of Standards and Technology, [en línea], Dirección URL:http://www.nist.gov/, [Consultado el 13 de enero 2013].

[89] Véase: Federal Information Security Management Act (FISMA), [en línea], SearchSecurity, Dirección URL:http://searchsecurity.techtarget.com/definition/Federal-Information-Security-Management-Act, [Consultado el 14 de enero 2013].

ser confidencialidad, para preservar las restricciones al acceso de información; en segundo lugar debe existir integridad entre las personas autorizadas a tener acceso a la información para evitar la modificación o destrucción de esta y en tercer lugar la no reproducción y autentificación de la misma y la disponibilidad, es decir que se garantice el acceso oportuno y confiable a la información[90]. Por ello, la FISMA se convierte en el marco de gestión y entendimiento que deben seguir todos los sistemas de información del gobierno federal para asegurar la información de todo el país. Para ello requiere que todas las agencias cuenten con un inventario de sus sistemas de información que cumplan con los requisitos mínimos de seguridad, aunque es importante destacar que existe flexibilidad en la implementación de controles de seguridad de las agencias dependiendo de su misión y entorno operativo, pero siempre cumpliendo con los Estándares Federales de Procesamiento (FIPS, siglas en ingles)[91] de Información del NIST.

2.1.3 Estrategia de Seguridad Nacional del Ciberespacio 2003

La Estrategia de Seguridad Nacional del Ciberespacio se creó con el fin de proteger contra el debilitamiento que afecta las operaciones de los sistemas de información de infraestructuras prioritarias y consecuentemente, ayudar a proteger tanto a la población como a la economía y a la seguridad nacional de los Estados

---

[90] Véase: Standards for Security Categorizations of Federal Information and Information Systems, 2004, [en línea], Department of Commerce, Dirección URL:http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf, [Consultado el 18 de enero 2013].

[91] Son estándares de procesamiento de información establecidos por el gobierno de los Estados Unidos para uso de las agencias no militares y contratistas del gobierno. Véase: Standards for Security Categorizations of Federal Information and Information Systems, *Ibidem.*

Unidos[92], a cargo del Departamento de Seguridad Nacional (DHS, siglas en ingles)[93], con coordinación entre el sector federal, estatal, local y el sector privado.

Los objetivos de esta estrategia eran prevenir ataques cibernéticos contra la infraestructura crítica de los Estados Unidos, reducir las vulnerabilidades nacionales y minimizar los daños frente a ataques cibernéticos. La Estrategia Nacional para proteger al ciberespacio delinea un marco para organizar y priorizar esfuerzos que tiene como principal función proveer de dirección a los departamentos del gobierno sobre su papel dentro del ciberespacio. Al mismo tiempo, sirve para identificar pasos que tanto el gobierno estatal y federal, las empresas privadas y organizaciones y ciudadanos norteamericanos deben desarrollar para mantener el espacio cibernético asegurado[94].

En esta estrategia se establecen cinco aspectos prioritarios para asegurar el ciberespacio que se encuentran plasmados en el Convenio sobre la Ciberdelincuencia, que se resumirán a continuación:

---

[92]Cita textual en ingles: *"protect against the debilitating disruption of the operations of information systems for critical infrastructures and, thereby, help to protect the people, economy, and national security of the United States".* The National Strategy to Secure Cyberspace, [en linea], Washington White House, February 2003, Dirección URL: https://www.us-Scert.gov/sites/default/files/publications/cyberspace_strategy.pdf, [Consultado el 23 de enero 2013].

[93] El 25 de noviembre de 2002 el Presidente George W. Bush creó el Departamento de Seguridad Nacional o Department of Homeland Security (DHS), constituido por 22 departamentos federales. Una de sus responsabilidades es proteger la seguridad del ciberespacio desarrollando planes nacionales para asegurar la infraestructura crítica; atender crisis frente a ataques; proveer de asistencia técnica al sector privado y otras dependencias ante emergencias en la infraestructura crítica y coordinarse con otras agencias para brindar información sobre peligros en los diversos sectores. Además, el Departamento de Seguridad Nacional se convirtió en el principal encargado de seguridad cibernética a nivel federal. Véase: *Ibidem,* p.10.

[94]Cita textual en inglés: *"The National Strategy to Secure Cyber Space outlines an initial framework for both organizing and prioritizing efforts. It provides direction to federal government departments and agencies that have roles in cyber space security. It also identifies steps that state and local governments, private companies and organizations, and individual Americans can take to improve our collective cyber security"* Lech J. Janczewski y Andrew M. Colarik, *Cyber Warfare and Cyber Terrorism*, Ed. Information Science Reference, Estados Unidos, 2008, p. 450.

1.- Un sistema de respuesta nacional de seguridad en el ciberespacio, requiere la cooperación entre el sector privado y el gobierno para compartir sus conocimientos, expandir el *Cyber Warning and Information Network* para manejar crisis, ampliar el sistema de alerta ante ciberataques y coordinación para el intercambio de información entre el sector público-privado.

2.- Un programa de reducción de amenazas y vulnerabilidades, requiere mejorar las capacidades de las fuerzas de seguridad, asegurar los mecanismos de Internet con protocolos, promover el uso de control digital seguro, conocimiento de amenazas y vulnerabilidades, priorizar la investigación en materia de ciberseguridad y asegurar sistemas emergentes.

3.-Formación y concientización en el ciberespacio, promover un entrenamiento enfocado en los ciudadanos, empresas, universidades y centros de investigación, el sector privado y el gobierno local y estatal.

4.-Asegurar el ciberespacio gubernamental, constante evaluación de las amenazas y vulnerabilidades de los sistemas cibernéticos, autentificar a los usuarios federales del sistema, asegurar la red *wireless* o inalámbrica.

5.-Cooperación nacional e internacional, debido a que los ciberataques cruzan fronteras territoriales, se necesita trabajar con organizaciones internacionales para establecer diálogos en materia de protección de infraestructura crítica, establecer una vigilancia internacional, así como alentar a los países a firmar el Convenio del Consejo de Europa sobre la ciberdelincuencia[95].

---

[95]Firmado en Budapest el 23 de noviembre de 2001, ratificado por Albania, Croacia, Estonia, Hungría, Rumania, Eslovenia y Macedonia. Tiene como prioridad proteger a la sociedad frente a la ciberdelincuencia, en el se tipifican los delitos (confidencialidad, informáticos, relacionados con el contenido, infracciones de propiedad intelectual), medios para combatir estos delitos y las sanciones. Véase: Convenio sobre la Ciberdelincuencia, [en línea], Dirección URL:http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Convention%20and%20protocol/ETS_185_spanish.PDF, [Consultado el 26 de enero 2013].

Estos cinco puntos hacen evidentes el reconocimiento por parte de la administración de George W. Bush de incluir tanto al sector público como al privado en la protección de la seguridad cibernética y la colaboración entre ellos y las organizaciones internacionales.

Esta Estrategia Nacional para Asegurar el Ciberespacio es uno de los primeros pasos para asegurar la infraestructura crítica de los Estados Unidos y destaca porque parte de la idea de crear una sociedad incluyente, donde todos los actores se encuentren involucrados en la ciberseguridad y por tal razón es necesaria la participación del gobierno federal, los gobiernos locales, de las empresas privadas y de la ciudadanía, postura que será ampliada durante la administración de Barack Obama.

Debemos destacar también que el creciente incremento de los problemas de ciberseguridad no solo afecta al Estado sino que traen consecuencias en distintos niveles, por lo cual se convierte no solamente en una amenaza para un país, sino para todo el mundo, debido a que este acelerado desarrollo tecnológico hace que todo el ciberespacio se vuelve vulnerable frente a una amenaza. Por ello se requiere de una estrategia que integre tanto la lucha contra el terrorismo como las vulnerabilidades del Estado dentro del ciberespacio.

2.1.4 Ley de Vigilancia de la Inteligencia Extranjera (FISA) 2008

La Ley de Vigilancia de Inteligencia Extranjera o *Foreing Intelligence Surveillance Act* (FISA, siglas en ingles) fue creada en 1978 por el presidente Nixon para espiar a grupos políticos opositores. Era la ley que regía los procedimientos de vigilancia electrónica y física de personas extranjeras.

En esta ley se requería la aprobación por parte de un tribunal para que las agencias de inteligencia obtuvieran órdenes de vigilancia y demostrar las razones específicas que justificaban la sospecha o participación en un delito dentro del territorio nacional o en el extranjero.

Sin embargo, durante la administración de George W. Bush en 2008 se realizó una enmienda a la FISA, cuyo principal objetivo seguía siendo la lucha contra el terrorismo, a la que se le denominó Ley de Enmiendas de FISA (FAA, siglas en ingles). Esta ley permitía a los servicios de inteligencia realizar espionaje de las comunicaciones electrónicas de ciudadanos estadounidenses con extranjeros supuestamente vinculados con el terrorismo, sin la necesidad de contar con una orden judicial, bajo la premisa de resguardar la seguridad nacional de los Estados Unidos. Esta enmienda a la FISA también eliminó los requisitos para investigar comunicaciones relacionadas con el extranjero.

2.1.2 El papel de las Agencias de inteligencia

Después del 11 de septiembre 2001 se mejoró la vigilancia contra el terrorismo incrementado de esta manera las actividades de las Agencias de Inteligencia, principalmente a la *National Security Agency* (NSA, siglas en ingles), *Central Intelligence Agency* (CIA, siglas en ingles) y Federal Bureau of Investigation (FBI, siglas en ingles), que endurecieron sus políticas de inteligencias. La política de George W. Bush frente a los servicios de inteligencia fue:

> *"[…] trasformar el potencial y construir uno nuevo que pueda mantenerse a la altura de la naturaleza de estas nuevas amenazas (…) Debemos fortalecer el poder de advertencia y de análisis del servicio de inteligencia para que proporcione valoraciones conjuntas sobre las amenazas a la seguridad de nuestra nación"*[96].

Gracias a esta visión las agencias de inteligencia instrumentaron como una de sus misiones la protección de la información enfocada en analizar amenazas,

[96]George W. Bush, "La estrategia de seguridad nacional de los Estados Unidos de América", *Revista Internacional de Filosofía Política*, México, Ed. UAM Iztapalapa, Julio 2003, No. 21, p. 233.

desarrollar guías, soluciones de seguridad, productos de cifra y gestión de claves, así como la formación y concentración de seguridad[97].

Un ejemplo de esto lo podemos ver con la orden ejecutiva secreta del presidente George W. Bush que autorizó a la NSA a realizar escuchas telefónicas sobre cualquier sospechoso de vínculos con el terrorismo, sin la necesidad de recurrir a una corte especial, como lo estipulaba el Acta de Vigilancia (FISA)[98], la cual como se señaló anteriormente implicaría posteriormente una modificación legislativa.

Estos programas de espionaje que antes eran solo utilizados para vigilar a otros países y a los extranjeros y que necesitaban la autorización de algunas autoridades para ser instrumentados, comenzaron a ser utilizados para vigilar a los ciudadanos estadounidenses. Sin embargo, se especula que los alcances fueron mayores porque incluyó la vigilancia de actividades de militares y élites políticas que antes eran inmunes a este tipo de vigilancia[99].

El gobierno de George W. Bush expandió los roles de la comunidad de inteligencia al monitoreo de las actividades en la red, como una medida de protección frente a futuros ataques en los sistemas cibernéticos de las agencias de intelgiencia[100]. Este proceso fue muy trascendente porque les dio a las agencias de inteligencia la posibilidad de contar con mayores posibilidades de vigilancia de las actividades

---

[97]Javier Candau Romero, *Estrategias Nacionales de Ciberseguridad. Ciberterrorismo*, *op.cit*. p.277.

[98] Cita textual en ingles: "*President George W. Bush issued a secret executive order authorizing the NSA to conduct phone-taps on anyone suspected of links with terrorism without the need to issue warrants from a special count, as required by the Foreign Intelligence Surveillance Act".*
Janczewski Lech J. y Colarik Andrew M., *op. cit*., p. 462.

[99] Cita textual en ingles: *"have also been turned inward by the National Security State against itself and targets military and political elites who long thought themselves immune from such close attention".* Burghardt Tom, *ECHELON Today: The Evolution of an NSA Black Program*, [en línea], Global Reserch, Julio 2013, Dirección URL: http://www.globalresearch.ca/echelon-today-the-evolution-of-an-nsa-black-program/5342646**,** [Consultado el 8 de octubre de 2013].

[100] Cita textual en ingles: *"expand the intelligence community's role in monitoring Internet traffic to protect against a rising number of attacks on federal agencies's computer systems".* Ellen Nakashima, *Bush Order Expands Network Monitoring*, [en línea], Washington Post, 26 de enero 2008, Dirección URL:http://www.washingtonpost.com/wp-dyn/content/article/2008/01/25/AR2008012503261.html, [Consultado el 8 de febrero de 2014].

realizadas en Internet (poder casi absoluto) sin la necesidad de requerir de una orden judicial por parte del gobierno para realizar esta labor. La justificación fue asegurar las redes gubernamentales contra intentos de inmiscuirse y poder anticipar amenazas[101]. Sin embargo, el tema fue polémico porque si bien se ha señalado que el Ejecutivo tiene capacidad de vigilancia con fines de inteligencia, no han quedado claras las atribuciones del Congreso en materia de vínculos entre vigilancia interna y externa.

El incremento de las funciones de espionaje de las agencias de inteligencia fue fuertemente cuestionado por la opinión pública. Las actividades de la NSA generaron entre los ciudadanos malestar, incluso algunos presentaron demandas por las actividades de vigilancia experimentadas, pero a pesar de ello las agencias del gobierno de los Estados Unidos justificaron sus actividades en términos de mantener la seguridad nacional frente al terrorismo y narcotráfico[102]. Sin embargo, las críticas difundidas por periódicos como el New York Times contribuyeron a que la ley estableciera diferencias de trato entre los extranjeros que viven fuera de Estados Unidos y los estadounidenses o extranjeros que viven en el país. Se acordó que para vigilar a un ciudadano estadounidense o un residente en el país, los servicios de inteligencia deben justificar su solicitud y obtener una orden judicial individual ante una corte secreta, pero los extranjeros residentes fuera del territorio nacional no disponen de estas protecciones constitucionales. Es decir, el Congreso dio a los espías prácticamente carta blanca para la vigilancia en el exterior, lo cual fue ratificado en el artículo 702 de la Ley FISA de 2008 que

---

[101]Cita textual en ingles: *"the president's directive represents a continuation of efforts to secure government networks, protect against constant intrusion attempts, address vulnerabilities and anticipate future threats".* Vocero de la Casa Blanca, Scott Stanzel, Ellen Nakashima, *Bush Order Expands Network Monitoring, Ibidem.*

[102]Cita textual en ingles: *"the capabilities and practices of the NSA have resulted in suspicion and resentment from overseas and U.S. citizens alike. Whether or not the methods employed by the NSA are legal, U.S. officials justify the NSA's activities as being necessary to acquire information about threats to national security, international terrorism and the narcotic trade",* Janczewski Lech J. y Colarik Andrew M., *op.cit.,* p. 463.

“otorga al gobierno nuevos poderes para controlar las comunicaciones de personas que se supone extranjeras y que viven fuera de Estados Unidos"[103].

Así podemos concluir que durante la administración del Presidente W. Bush, los servicios de inteligencia adquirieron mayor relevancia al convertirse en pilares defensivos, para establecer las bases de una política preventiva contra el terrorismo y las amenazas hostiles del exterior. Ello significó el fortalecimiento de su autoridad y sus capacidades para que su intervención fuera más funcional y oportuna frente a las amenazas, pero también significó a nivel de política internacional que prevaleciera una visión de unipolaridad como factor condicionante de la política exterior norteamericana, lo cual reforzó la noción de superioridad sobre el resto del mundo.

El proceso de constante vigilancia de comunicaciones telefónicas y electrónicas en busca de conexiones con redes terroristas debilitó los derechos de los ciudadanos en materia de privacidad, lo cual generó fuertes controversias internas.

Finalmente, no obstante, que el gobierno priorizó en materia de seguridad nacional la lucha contra el terrorismo, descuidó algunas áreas y dejó de lado la política de concientización de la importancia de la ciberseguridad[104].

---

[103]AFP, *El casi desconocido artículo 702 que permite a EE.UU. espiar a internet*, [en línea], El País, 11 de junio 2013, Dirección URL: http://www.elpais.com.uy/mundo/articulo-eeuu-epiar-internet.html, [Consultado el 10 de mayo de 2014].

[104]Cita textual en ingles: *“while the government is moving to coordinate intergovernmental security arrangements, even in the security arena coordination with the private sector needs much more active consideration”.* Capítulo I Cyberpower and National Security: Policy Recommendations for a Strategic Framework, en Franklin D. Kramer, Stuart H. Starr y Larry K. Wentz (editors),*Cyberpower and National Security*, Washington D. C., Center for Technology and National Security Policy/National Defense University Press/Potomac Books Inc., p. 11.

2.2 Administración de Barack Obama (2009-2013)

La administración de Barack Obama[105] se ha caracterizado por establecer diversas medidas para enfrentar las amenazas cibernéticas, al considerar que éstas tienen repercusiones económicas y políticas que afectan directamente a los intereses nacionales de los Estados Unidos y de sus principales aliados.

Se ha buscado la intervención del sector privado y el público en este proceso y la constante evaluación de las medidas de seguridad. Se han definido las vulnerabilidades y se ha buscado crear una concientización de la importancia del ciberespacio, alentando la investigación y el desarrollo de nuevas medidas de seguridad cibernéticas. Se busca generar conexiones a Internet más seguras y un monitoreo contante de la información que circula por el ciberespacio.

Esta postura la podemos ver claramente en un comentario hecho por el Presidente Barack Obama quien declaró que:

> *"[…] dado el enorme daño que puede causar incluso un único ataque cibernético, no bastará con respuestas a medida no es suficiente el reforzar nuestra defensa tras los incidentes o ataques. De igual forma a cómo hacemos frente a los desastres naturales, hemos de tener planes y recursos de antemano, compartiendo información, emitiendo avisos y asegurando una respuesta coordinada"*[106].

Lo cual demuestra que la administración Obama a partir del reconocimiento de sus vulnerabilidades ha centrado sus esfuerzos en materia de políticas de seguridad informática y en el desarrollo e investigación de nuevas tecnologías. Considera

---

[105]Barack H. Obama nació en Hawai en 1961. Estudió leyes en la Universidad de Columbia y en Harvard Law School, donde fue presidente de Harvard Law Review. Fue senador por el estado de Illinois en 2005. Fue elegido como 44 Presidente de los Estados Unidos por el partido demócrata a partir del 20 de enero de 2009. El 6 de noviembre del 2012 el presidente Barack Obama fue reelegido para un periodo de cuatro años más. Véase: http://www.whitehouse.gov/espanol/presidente-obama/, [Consultado el 10 de febrero de 2014].

[106]Presidente Barack Obama, 29 de mayo 2009, p. 224, Dirección URL: http://bibliotecavirtualdefensa.es/BVMDefensa/i18n/catalogo_imagenes/grupo.cmd?path=17029, [Consultado el 10 de febrero de 2014].

que la prosperidad de la economía de los Estados Unidos dependerá de la implementación de políticas de ciberseguridad, ya que es un elemento indispensable para que el país pueda continuar con el crecimiento de la economía nacional y de esta manera mantener su estilo de vida[107].

Por tales razones la administración del Presidente Barack Obama nombró a Howard Schmidt[108] como Coordinador de Seguridad Cibernética y creó la Oficina de Seguridad Cibernética en el Estado Mayor de Seguridad Nacional, para que trabajara en estrecha colaboración con el Director de Información Federal, Steven VanRoekel, con el Director Federal de Tecnología, Todd Park y con el Consejo Económico Nacional.

Durante el mandato de Barack Obama se han incrementado las políticas de ciberseguridad, con iniciativas como la de 2009 *The Comprehensive National Cybersecurity*[109], en donde el Departamento Seguridad Nacional adquiere mayores responsabilidades coordinando el ámbito federal, estatal, local y vinculando el aspecto privado con el público.

Sus principales estrategias según Javier Candau Romero son las siguientes:

1. Generar un sistema de respuesta nacional de seguridad en el ciberespacio. A través de la mejora de la gestión de incidentes, ampliar el sistema de alerta ante ciberataques, realizar ejercicios de coordinación o mejorar el intercambio de información público-privado.

---

[107] Cita textual en ingles: "*We must secure our cyberspace to ensure that we can continue to grow the nation's economy and protect our way of life"* .Véase: Cybersecurity, White House, Dirección URL :http://www.whitehouse.gov/issues/foreign-policy/cybersecurity, [Consultado el 11 de febrero de 2014].

[108] Ex jefe de seguridad de Microsoft, conocido como el zar de la seguridad para la administración de Barack Obama.

[109]*The Comprehensive National Cybersecurity Initiative,* Estados Unidos, 2009, [en línea], Dirección URL:http://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative, [Consultado el 18 de febrero de 2014].

2. Programa de reducción de amenazas y vulnerabilidades. Por medio de la mejora de las capacidades de las fuerzas de seguridad (FBI) y otras agencias policiales del control de los sistemas SCADA (siglas en ingles) o profundizar en el conocimiento sobre amenazas y vulnerabilidades.

3. Formación y concienciación en el ciberespacio. Para ciudadanos y pequeñas empresas, empresas consideradas estratégicas, universidades y centros de investigación (especialmente los que dispongan de gran capacidad de cálculo), sector privado (especialmente el que disponga de sistemas SCADA) y gobiernos locales y estatales.

4. Asegurar el ciberespacio gubernamental, para implementar las mejoras de seguridad necesarias.

5. Cooperación nacional e internacional, reforzar las actividades de contrainteligencia con las diferentes agencias, a través de mejorar los canales de comunicación y las medidas a legislativas nacionales[110].

La estrategia de Barack Obama mostró un cambio frente a Bush, no estableció como principal objetivo la lucha contra el terrorismo sino que reconoció la vulnerabilidad del Estado y del sector privado en el ciberespacio.

Señaló que la falta de seguridad de este espacio puede provocar que cualquier persona interna o externa entre en la red y la tire, lo cual podría traer graves consecuencias económicas, políticas, sociales y diplomáticas no sólo para los Estados Unidos sino para todo el mundo.

Así, Obama estableció una estrategia que englobaba a diferentes actores y una estrecha coordinación entre los elementos militares, civiles y de seguridad.

[110]Javier Candau Romero, *Estrategias Nacionales de Ciberseguridad. Ciberterrorismo*, en Ministerio de Defensa de España, Ciberseguridad. Retos y amenazas a la Seguridad Nacional en el ciberespacio, *op.cit.,* Pp. 275-276.

Priorizó el resguardo de información, actualización, así como la capacitación de la población para evitar que estas amenazas generen graves consecuencias. Las razones por las cuales el gobierno de Barack Obama priorizó las políticas de seguridad cibernéticas fueron por un lado las críticas hacia el sexenio anterior que abandonó este aspecto y el contexto desfavorable en que inició su administración, debido a que se dieron a conocer los documentos de los *Cablegates* de Wikileaks, lo que le generó fuertes presiones en materia de seguridad cibernética.

2.2.1 Creación del Comando Cibernético (CYBERCOM) 2010

El 21 de mayo de 2010 se estableció el Comando Cibernético de los Estados Unidos (CYBERCOM, siglas en ingles) a cargo del general Keith Alexander quien consideraba que la guerra cibernética utiliza al ciberespacio para atacar al personal, las instalaciones o equipos con la intención de degradar, o destruir la capacidad de combate del enemigo, mientras se protege la propia[111].

Su misión era planear, coordinar e integrar las actividades para defender la red de información del Departamento de Defensa y conducir operaciones militares en el ciberespacio como medida para asegurar la libertad de acción de los Estados Unidos dentro del ciberespacio.

Este Comando Cibernético[112] se creó con la finalidad de mejorar las capacidades del Departamento de Defensa para asegurar las redes, contar con información fiable, comunicación segura en el ciberespacio, que sería de apoyo para que las Fuerzas Armadas, pudieran generar seguridad de alto nivel, a través de

---

[111] Cita textual en ingles: *"the focus of cyber warfare is on using cyberspace to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability, while protecting our own".* Franklin D. Kramer, Stuart H. Starr y Larry K. Wentz, *Cyber power and National Security,* o*p.cit*, p. 14.

[112] Este Comando Cibernético tiene tres principales misiones: la protección diaria de las redes de defensa; establecer una única cadena de comando dirigida por el presidente y trabajar en alianza para compartir información sobre amenazas y ayudar a generas respuestas coordinadas.

operaciones efectivas, comandos de protección, control de los sistemas y aseguramiento de la infraestructura crítica frente a amenazas.

El CYBERCOM se subdivide en el Comando Estratégico de los Estados Unidos (USSTRATCOM, siglas en ingles), el Comando Cibernético del Ejército (FLTCYBERCOM, siglas en ingles), el Comando Cibernético de la Flota (FLTCYBERCOM, siglas en ingles) y las Comando Cibernético de las Fuerzas de la Marina (MARFORCYBER, siglas en ingles)[113].

El gobierno de Barack Obama consciente de la gran amenaza que significaba para su país una guerra cibernética, declaró a la infraestructura digital como un activo estratégico nacional, para lo cual nombró a Howard Schimidt , ex jefe de seguridad de Microsoft (como zar de la ciberseguridad) y al General Keith Alexander director de la Agencia Nacional de Seguridad (NSA), con el objetivo de "conducir las operaciones de amplio espectro para defender las redes militares de Estados Unidos y los ataques si fuera necesario a los sistemas de otros países"[114].

William J. Lynn, Subsecretario de Defensa, expuso que los cinco principios básicos de la estrategia de guerra en el futuro serán el ciberespacio como el quinto dominio de los Estados al igual que la tierra, mar, aire y espacio. Por lo cual se debe establecer la defensa del ciberespacio más allá de las redes militares (dominio.mil y .gov) sino hasta las redes comerciales (dominio.com; .net; .info;

---

[113] US. Cyber Command Fact Sheet, [en línea], US Department of Defense, 25 de mayo de 2010, Dirección URL:http://www.defense.gov/home/features/2010/0410_cybersec/docs/CYberFactSheet%20UPDATED%20replaces%20May%2021%20Fact%20Sheet.pdf, [Consultado el 10 de febrero de 2014].

[114] Ministerio de Defensa de España, *Ciberseguridad, Retos y amenazas a la seguridad nacional en el ciberespacio*, o*p. cit.,* p. 21.

.edu) que deben estar también subordinados al concepto de Seguridad Nacional para lo cual se necesita de la cooperación de las empresas privadas[115].

Para esta defensa ciberespacial plantea también el establecimiento de alianzas internacionales con una política de alerta compartida; el Departamento de Defensa debe incrementar el dominio tecnológico de los Estados Unidos, para mantenerse al día con la gran evolución de las tecnologías[116]. Debido a que hasta ese momento "el Cibercomando protege solo al dominio militar <.mil>. El dominio de gobierno <.gov> y el de infraestructuras corporativas como <.com> son responsabilidad respectivamente del *Departament of de Homeland Security* y de las empresas privadas con apoyo de Cybercom"[117].

2.2.2 Iniciativa de Seguridad Cibernética Nacional Integral (CNCI, siglas en ingles)

En 2009 tras asumir el cargo presidencial, Barack Obama ordenó una revisión exhaustiva de los esfuerzos federales para defender la infraestructura de información y comunicaciones de los Estados Unidos. Ello derivó en varias recomendaciones que incluían una colaboración con todos los actores clave en la ciberseguridad, tanto gobiernos estatales, locales y el sector privado, para garantizar una respuesta organizada y unificada en futuros incidentes cibernéticos, fortalecer las alianzas público/privadas, invertir en la investigación de vanguardia, establecimiento de un responsable de ciberseguridad en las diferentes agencias, actualizar la estrategia para proteger la infraestructura crítica, ciberseguridad como prioridad gubernamental, designar un responsable de privacidad en el Consejo de

---

[115] Luis Joyanes Aguilar, Introducción. Estado del Arte de la Ciberseguridad, en Ministerio de Defensa de España, *Ciberseguridad, Retos y amenazas a la seguridad nacional en el ciberespacio*, Diciembre 2010, Pp. 30 y 31. [en línea], Dirección URL:http://bibliotecavirtualdefensa.es/BVMDefensa/i18n/catalogo_imagenes/grupo.cmd?path=17029, [Consultado el 28 de enero de 2014].

[116] William J, Lyns, *Defending a New Domain - The Pentagon's Cyberstrategy*,.Foreign Affairs, Num. 5, Vol. 89, septiembre/octubre de 2010, p. 97.

[117] Ciberseguridad, Retos y amenazas a la seguridad nacional en el ciberespacio, *op. cit*., p. 33.

Seguridad Nacional (NSC, siglas en ingles), realizar políticas de coordinación en las diferentes agencias, hacer campañas nacionales de concientización, preparar planes de respuesta frente a incidentes, mejorar las capacidades de investigación y asegurar la privacidad[118].

Estas recomendaciones derivaron en la reformulación de la Iniciativa Nacional Integral de Seguridad Cibernética (CNCI), lanzada por el presidente George W. Bush en enero de 2008. El Presidente Obama determinó desde mayo de 2009 que era necesario crear una nueva estrategia de seguridad cibernética para los Estados Unidos, por lo que con ayuda de su jefe de ciberseguridad, Michael Daniel[119] esta iniciativa sería el eje de su política sobre este tema.

La CNCI consiste en 12 iniciativas para ayudar a proteger a Estados Unidos en el ciberespacio a través de una línea de defensa contra las amenazas inmediatas mediante la mejora de las vulnerabilidades de la red y la capacidad de actuar con rapidez y prevenir intrusiones. Defender el espectro de amenazas mejorando las capacidades de contrainteligencia, el aumento de la seguridad, educación cibernética y coordinar esfuerzos de investigación entre el Gobierno Federal y el sector privado para desarrollar estrategias que disuadan la actividad hostil en el ciberespacio.

Para cumplir estos objetivos se necesita el apoyo de las agencias de inteligencia para mejorar la recolección de inteligencia, el procesamiento y análisis, así como el aseguramiento de la información fundamental. Sin embargo, para que los

---

[118]Cyberspace Policy Review, [en línea], White House, Dirección URL: http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf, [Consultado el 18 de febrero de 2014].

[119] Encargado del desarrollo interinstitucional de la estrategia nacional de ciberseguridad, la supervisión de estas políticas en las agencia, al igual que supervisa la colaboración entre el sector privado y el gobierno federal. Véase: Michael Daniel, [en línea], White House, Dirección URL :http://www.whitehouse.gov/blog/author/Michael%20Daniel, [Consultado el 20 de febrero de 2014].

esfuerzos nacionales de ciberseguridad sean exitosos se requiere que se basen siempre en la protección de los derechos civiles y la privacidad[120].

A continuación se presenta un cuadro con un resumen de los objetivos de cada iniciativa instrumentadas por el gobierno de los Estados Unidos con la finalidad de clarificarlos:

Tabla 1 Iniciativas de Seguridad Cibernética Nacional Integral

No	Iniciativa	Objetivo / propósito
1	**Gestionar las Empresas Federales de Redes como una sola empresa de red con Conexiones a Internet de confianza** Iniciativa de las Conexiones a Internet de Confianza (TIC por sus siglas en inglés)	Brindar soluciones de seguridad común para reducir los puntos de acceso externos. Establecer capacidades de seguridad y adhesión de agencia como proveedores o la contratación de proveedores comerciales. Crear Servicios Gestionados de Protocolos de Internet de Confianza (MTIPS, siglas en ingles) a través de la NETWORX vehículo contrato por la Administración de Servicios Generales (GSA).
2	**Implantar un sistema de detección de intrusiones de sensores en la empresa federal** (EINSTEIN 2)[121]	Identificar usuarios no autorizados que pretenden ingresar a las redes gubernamentales. Inversión en el programa DHS. EINSTEIN 2 capaz de alertar a *United State Computer Emergency Readiness Team* (US-CERT) en tiempo real.
3	**Continuar el despliegue de los sistemas de prevención de intrusiones en la empresa federal.** (EINSTEIN 3)[122]	EINSTEIN 3 Identificar automáticamente y caracterizar amenazas antes de que causen un daño, proporcionando un sistema de prevención de intrusiones. Asistir al US-CERT en el intercambio de información. El intercambio de información se llevará a cabo de conformidad con las leyes con el

[120] The Comprehensive National Cybersecurity Initiative, White House, [en línea], Dirección URL : http://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative, [Consultado el 18 de febrero de 2014].

[121] EINSTEIN 2 fue integrado en 2008, como un sistema autómata que incorpora la detención de intrusos basada en firmas personalizadas de amenazas conocidas.

[122]EINSTEIN 3 es un servicio de seguridad administrado por el Departamento de Seguridad Nacional y proveedores de Internet, que funciona contra protección de intrusiones y prevención, desplegado por primera vez en 2004 que ha evolucionado hasta analizar el tráfico dentro de la red y bloquear automáticamente las amenazas. William Jackson, *Eisntein 3 goes live with automated malware blocking*, [en línea], GCN, 24 de Julio 2013, Dirección URL: http://gcn.com/articles/2013/07/24/einstein-3-automated-malware-blocking.aspx, [Consultado el 20 de febrero de 2014].

		fin de proteger la privacidad de los ciudadanos estadounidenses.
4	**Coordinar y redirigir los esfuerzos de Investigación y Desarrollo (I y D)**	Estrategias de coordinación de las actividades de desarrollo e investigación del gobierno de los Estados Unidos. Para eliminar investigaciones no funcionales e identificar las lagunas en la investigación.
5	**Conectar centros cibernéticos para mejorar la conciencia de la situación actual**	Colaboración en 6 centros que monitorean las capacidades fundamentales y las inversiones como infraestructura mejorada. Incrementar la banda ancha, las capacidades operacionales integradas; mejorar la colaboración, mayor conocimiento de la situación compartida a través de análisis compartido y la colaboración en tecnologías.
6	**Desarrollar e instrumentar un plan de ciber contra inteligencia (CI)**	Coordinar actividades dentro de las agencias federales de inteligencia para detectar, desalentar y mitigar amenazas cibernéticas externas. Educación de contrainteligencia, programas de sensibilización y desarrollo de fuerza laboral, aumentando así la conciencia de la amenaza cibernética. Alineado con la Estrategia Nacional de Contrainteligencia de los Estados Unidos de América (2007)[123].
7	**Aumentar la seguridad de las redes clasificadas**	Mejorar la seguridad para evitar la filtración de información delicada que pueda causar daños graves a la seguridad nacional.
8	**Ampliar la educación cibernética**	Incentivar la educación en materia cibernética para generar mano de obra calificada y ciber-inteligente dentro del Gobierno Federal.
9	**Definir y desarrollar tecnologías, estrategias y programas a largo plazo**	Generar estrategias y programas para solucionar problemas de alto riesgo/alta rentabilidad a 5 y 10 años.
10	**Definir y desarrollar estrategias duraderas y programas de disuasión**	Mejora las capacidades de alerta, la articulación de roles para el sector privado y los asociados internacionales, y desarrollar respuestas apropiadas
11	**Desarrollar un enfoque múltiple por la gestión de riesgos en la cadena de suministro global**	Mayor concientización de las amenazas, vulnerabilidades y consecuencias de un ataque. Desarrollo de nuevas políticas de adquisiciones y prácticas y la asociación con la industria para desarrollar y adoptar la cadena de suministro

[123] La Estrategia Nacional de Contrainteligencia de los Estados Unidos, es un medio para proteger la defensa de la tecnología crítica, ya que ayuda a proteger secretos tecnológicos.

12	**Definir el papel del gobierno federal para la ampliación de la seguridad cibernética en dominios de infraestructura crítica**	Desarrollar estrategias entre el gobierno federal y el sector privado para establecer una estrategia integral, recomendaciones a corto plazo como a largo plazo.

Elaboración propia, con base en The Comprehensive National Cybersecurity Initiative, White House, Dirección URL: http://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative, [Consultado el 23 de febrero de 2014].

En la elaboración de esta estrategia observamos que el Presidente Barack Obama llegó a la conclusión de que no era suficiente establecer políticas de ciberseguridad sólo con las instituciones públicas, sino que se necesitaba establecer una alianza entre el sector público y el privado para proteger esta infraestructura crítica. Sin embargo, el sector privado se mantuvo renuente a sumarse, porque en este sector prevalecía una visión de competencia entre empresas más que de apoyo y colaboración con el gobierno.

También se dificultó el establecimiento de alianzas internacionales porque de igual manera cada país prioriza su seguridad estatal y no existen acuerdos sobre lineamientos generales. Además de que aún falta a nivel internacional conciencia sobre la importancia y los riesgos que tiene el ciberespacio para los diferentes sectores y para los estados, lo cual dificulta la investigación y la innovación en materia de seguridad de manera conjunta.

2.2.3 Ley Nacional de Activos para Proteger el Ciberespacio

En 2010 se estableció la *Protecting Cyberspace as a National Asset Act* o Ley Nacional de Activos para Proteger el Ciberespacio como una medida para resguardar la infraestructura crítica norteamericana, incrementando las capacidades de alerta temprana en tiempo real. Implicaba también la creación de dos oficinas de ciberseguridad una dentro de la Casa Blanca y otra en el Departamento de Seguridad Nacional.

La primera supervisaría las actividades del ciberespacio y desarrollaría estrategias de ciberseguridad nacional, para fortalecer la capacidad de recuperación del ciberespacio, supervisar y coordinar las políticas federales en materia de ciberseguridad, asegurarse que todas las agencias federales cumplan con las directrices del Departamento de Seguridad Nacional[124].

La segunda en el Centro Nacional de Ciberseguridad y Comunicaciones (NCCC, siglas en ingles) para proteger tanto el dominio público y el privado[125] con lo cual se modernizó la Ley de Gestión de Seguridad de la Información Federal (FISMA) y brindó la posibilidad de que cualquier infraestructura crítica dentro de los Estados Unidos ya sea de empresas privadas o de sistemas telefónicos sea analizada por este Centro de Investigación.

Esta ley permite que el Presidente de los Estados Unidos, en caso de una emergencia que pueda generar graves daños o pérdidas humanas, autoriza desconectar tanto la red gubernamental como la red privada dentro de Internet[126] para lo cual requiere de la aprobación por parte del Congreso.

Finalmente, la ley también se creó para que las empresas privadas no tengan la necesidad de tener que tomar medidas extremas en situación de emergencia, frente a una amenaza que pueda afectar su infraestructura crítica, sino que sea la propia estructura gubernamental la responsable.

---

[124]Protecting Cyberspace as a National Asset Act of 2010, Official Summary, [en línea], Open Congress, Dirección URL:http://www.opencongress.org/bill/111-s3480/show, [Consultado el 26 de febrero de 2014].

[125] Véase Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio, o*p. cit.* Pp. 68-70.

[126]Cita textual en ingles: *"emergency authorithy to shut down prívate sector or government networks in the event of a cyber attack capable of causing massive damage or loss of life"* Bianca Bosker, *Internet 'Kill Switch' Approved by Senate Homeland Security Committee*, [en línea], Huffington Post, 25 de junio de 2010, Dirección URL:http://www.huffingtonpost.com/2010/06/25/internet-kill-switch-appr_n_625856.html, [Consultado el 12 de febrero de 2014].

2.2.4 Estrategia de Ciberseguridad 2013

La estrategia de ciberseguridad del Presidente Barack Obama en 2013 se caracterizó por seguir dos principios: mejorar la capacidad de resistencia a los incidentes cibernéticos y reducir las amenazas cibernéticas. Para mejorar la capacidad de resistencia cibernética, se establecieron políticas que incluían el endurecimiento de la infraestructura digital para evitar penetraciones. El objetivo era mejorar la defensa contra las amenazas cibernéticas sofisticadas y ágiles así como la rápida recuperación de los incidentes.

Estos objetivos se alcanzarían a través de la colaboración con los aliados que contribuirían a definir normas internacionales de comportamiento aceptable en el ciberespacio, el fortalecimiento de las capacidades de aplicación de la ley contra los delitos informáticos, y disuadir a potenciales adversarios de tomar ventaja. Para lo cual era importante que el gobierno de los Estados Unidos tuviera información real del estado de las redes, así como las capacidades e intenciones de sus enemigos cibernéticos, lo cual debe ser conocido por todos los funcionarios defensores de la seguridad cibernética.

En el documento *Cyberspace Policy Review* el gobierno de Obama identificó 10 acciones a corto plazo para mejorar la estrategia de seguridad cibernética que consisten en: 1) una política oficial de la ciberseguridad que coordine las políticas y acciones de seguridad cibernética; 2) crear una estrategia nacional actualizada para asegurar la información y la infraestructura de comunicaciones; 3) designar prioridades clave y establecer parámetros de rendimiento; 4) designar un funcionario encargado de la seguridad cibernética; 5)crear análisis interinstitucional de prioridades de la ciberseguridad; 6) iniciar una campaña nacional de sensibilización y educación para promover la ciberseguridad; 7) desarrollar un marco internacional de políticas de ciberseguridad y fortalecer alianzas internacionales; 8) preparar un plan para responder a incidentes e iniciar un diálogo para mejorar las asociaciones público-privadas; 9) desarrollar nuevas

tecnologías para mejorar la infraestructura crítica digital; 10) construir una identidad de gestión basada en la seguridad cibernética y el aprovechamiento de las tecnologías[127].

La postura de Barack Obama durante 2013 fue firmar una orden ejecutiva que fortaleciera la ciberdefensa a través de incrementar la información compartida y desarrollar estándares que protejan la seguridad nacional y la privacidad. Demandó al Congreso colaborar en esta tarea generando leyes que ayuden a asegurar la red cibernética[128].

2.2.5 El papel de las Agencias de Inteligencias en el mandato de Barack Obama

Ha sido muy cuestionado el papel de las agencias de inteligencia durante la administración de Barack Obama porque con el establecimiento de políticas de seguridad cibernética obtuvieron mayores atribuciones de funcionamiento que durante el régimen de Bush. No sólo han interceptado mensajes telefónicos y correos electrónicos, sin orden judicial, de personas sospechosas de terrorismo, sino incluso de personas no inculpadas y los límites entre ciudadanos norteamericanos y extranjeros se perdieron en la práctica política.

Se generó polémica en torno al presupuesto que la administración de Obama destinó a las agencias de inteligencia, ya que solo un pequeño grupo de legisladores tiene acceso al presupuesto destinado a este rubro, lo que llevó a

---

[127]Véase: Cybersecurity, White House, Febrero 2013, [en línea], Dirección URL: http://www.whitehouse.gov/issues/foreign-policy/cybersecurity, [Consultado el 26 de febrero de 2014].

[128]Cita textual en ingles: "*signed a new executive order that will strengthen our cyberdefenses by increasing information sharing, and developing standarsds to protect our national security, our jobs and our privacy But now, Congress must act as well, by passing legislation to give our government a greater capacity to secure our networks and deter attacks This is something we should get done on a bipartisan basis"* Erick Chabrow, *Obama Issues Cybersecurity Executive Order*, [en línea], Gov Info Security, Febrero 2013, Dirección URL:http://www.govinfosecurity.com/obama-issues-cybersecurity-executive-order-a-5506, [Consultado el 28 de febrero de 2014].

plantear la necesidad de controlar y transparentar la labor de las agencias de inteligencia. Algunos periódicos como Washington Post evidenciaron que se estaba destinando aproximadamente $14.7 billones de dólares a la CIA, mientras que la NSA recibía $10.8 billones y $10.3 billones la Oficina de Reconocimiento Nacional, agencia dedicada a la operación de espías satelitales para el año 2013[129].

También se generó gran controversia porque durante la administración de Obama se dieron a conocer las filtración de información clasificada por parte de Wikileaks, lo cual mostró las políticas de espionaje, que mantenía el gobierno de los Estados Unidos sobre los gobernantes de otras naciones y sus propios ciudadanos, a través de escuchas telefónicas y revisión de correos electrónicos.

Por otra parte, la administración de Obama desde finales de 2013 presentó una iniciativa para reformar las políticas de espionaje, la cual incorporó el compromiso de analizar las políticas de inteligencia de manera anual, trasparentar las actividades realizadas en esta materia y establecer límites en la acumulación de registros telefónicos, precisando las razones para espiar[130]. De llevarse a cabo esta reforma sería un importante cambio en la política de espionaje, porque sería un primer paso para lograr una rendición de cuentas, la cual a mediano plazo podría significar regulaciones más claras en la materia. Sin embargo, aún hoy en día el tema está a debate.

---

[129] Cita textual en ingles: *"the C.I.A. ($14.7 billions last year) and the N.S.A. ($10.8 billions). The third-highest budget went to an agency most Americans have never heard of: the National Reconnaissance Office, which build and operates spy satellites and cost $10.3 billion last year."* David Firestone, Why are the Intelligence Budgets a State Secret?, [en línea], The New York Times, 17 de enero de 2014, Dirección URL:http://takingnote.blogs.nytimes.com/2014/01/17/why-are-the-intelligence-budgets-a-state-secret/?ref=centralintelligenceagency, [Consultado el 1 de marzo de 2014].

[130] Véase *Obama anunció cambios a la política de espionaje de la NSA*, [en línea], Univision Noticias, 17 de enero de 2014, Dirección URL:http://noticias.univision.com/article/1819820/2014-01-17/estados-unidos/noticias/obama-anunciara-cambios-en-la-nsa, [Consultado el 28 de febrero de 2014].

Por otra parte, Wikileaks puso a discusión otro gran problema en el funcionamiento de las agencias de inteligencia su falta de autosuficiencia para resolver sus problemas de procesamiento de información y de apoyo tecnológico. Frente a esta situación recurrieron a la subcontratación de empresas privadas. Debido a que las Agencias se vieron rebasadas por los avances tecnológicos en telecomunicaciones y en Internet, agencias como la NSA tuvieron que recurrir al sector privado para contratar infraestructura actualizada para monitorear la información. Ello significó que empresas privadas comenzaran a realizar trabajos esencialmente gubernamentales. Adicionalmente, el proceso resultó muy costoso a largo plazo, ya que de acuerdo con algunas estimaciones el 70% del presupuesto de inteligencia se ha destinado al pago del sector privado[131].

Finalmente, otro problema de esta subcontratación es que se creó una cadena de personal con acceso a información clasificada, que no sigue los estándares de confidencialidad y seguridad que deben mantener las agencias de inteligencia. Este personal no tiene que pasar por la supervisión del Congreso y sólo rinde cuentas a las compañías que los contrataban, lo cual generó vulnerabilidad en el manejo de la información, como lo mostró Wikileaks.

La subcontratación de empresas privadas dentro de las agencias de inteligencia es un tema controvertido porque requiere de un cambio estructural, así como del establecimiento de políticas claras en esta materia para evitar que estas empresas privadas ponga en riesgo la seguridad nacional con la fuga de información clasificada.

---

[131] Cita textual en ingles: "*we have government contractors doing what are essentially governmental jobs, (…) Seventy percent of America's intelligence budget now flows to private contractors"* Tim Shorrock, *Put the Spies back under one roof,* [en línea], Estados Unidos, The New York Times, The Opinion pages, 17 de junio 2013, Dirección URL:http://www.nytimes.com/2013/06/18/opinion/put-the-spies-back-under-one-roof.html?ref=centralintelligenceagency, [Consultado el 25 de febrero de 2014].

2.2.6 Éxitos y fracasos de los reajustes de las políticas de seguridad informática de Estados Unidos

Aunque durante la administración de Barack Obama se han instrumentado diversas políticas para asegurar la infraestructura crítica, estas han sido limitadas porque continúan observándose debilidades frente a un ataque cibernético. Uno de los problemas es la falta de desarrollos tecnológicos en el sector gubernamental o en las agencias, lo cual obliga a la alianza estratégica con las empresas privadas se vuelva prioritaria[132]. Sin embargo, también tienen que resolverse los problemas propios de esa vinculación, así como los mecanismos de control para evitar fugas de información y las confrontaciones entre los propios competidores.

Una de las bases de estas políticas de seguridad fue establecer una cooperación con aliados claves sobre información trascendental en materia de seguridad cibernética, pero esto genera un importante cuestionamiento sobre cuál es la información que puede ser compartida cuando está en juego la seguridad nacional, pero también sobre las ganancias económicas por parte de las empresas cibernéticas.

Aunque el gobierno de los Estados Unidos reconoce la relevancia de la seguridad cibernética, las medidas implementadas no han logrado solucionar el conflicto dentro del ciberespacio, porque los diferentes actores involucrados tienen posturas, prioridades e intereses diferentes sobre la ciberseguridad y sobre las amenazas, lo cual dificulta más el resguardo de este dominio.

---

[132]Cita textual en ingles: *"despite these initiatives, U.S. policy still lacks a coherente approach to protecting critical digital assets outside of the government and, in most cases, relies on the voluntary participation of private industry"* Jonathan Master, *Confronting the Cyber Threat,* [en línea], Council on Foreign Relations, 23 de mayo de 2013, Dirección URL: http://www.cfr.org/technology-and-foreign-policy/confronting-cyber-threat/p15577, [Consultado el 3 de marzo de 2014].

En conclusión podemos decir que las administraciones de George Bush y Barack Obama centraron sus esfuerzos en instrumentadar diversas medidas legislativas para asegurar el ciberespacio y establecer alianzas entre el sector privado, público y las universidades. Además fortalecieron a las agencias de inteligencia, como medidas para proteger la Seguridad Nacional. Sin embargo, esto no resolvió el problema de la seguridad de la información porque estas acciones se centraron en mejorar los lineamientos estructurales, pero descuidaron los mecanismos de operación de las agencias de inteligencia.

Asimismo estas adquirieron mayor autonomía para vincular a la comunidad universitaria y las principales empresas de los sectores de las telecomunicaciones e Internet como medida para contar con capital humano bien capacitado. Sin embargo, esta relación de tres bandas no ha permanecido estable en el tiempo, sino que ha evolucionado siguiendo las dinámicas conectadas con el desarrollo tecnológico. Ello ha llevado a la vinculación con empresas que no nacieron bajo el paraguas de la comunidad de inteligencia o de defensa, por lo que la confianza y la capacidad de control directo o indirecto de estos contratistas es también menor, lo que abrió espacio para la filtración de información. El ciberespacio se ha convertido en una zona estratégica para los intereses norteamericanos, pero las filtraciones también mostraron que el ciberspacio no es un bien común abierto y seguro para el usuario, sino un espacio utilizado para obtener poder e información por parte del propio gobierno en alianza con grupos privados.

Capítulo 3 La filtración de los *Cablegates* de Wikileaks. Consecuencias internas

El gobierno norteamericano ha enfrentado varios obstáculos para preservar su seguridad nacional dentro del ciberespacio, debido a que con la revolución tecnológica se ha incrementado el número de usuarios y de actividades en la red, lo cual generó una saturación en la capacidad del Estado para monitorear de cerca la información que circulaba dentro de la red[133].

Adicionalmente, fallas en los sistemas y programas tecnológicos, pueden poner en riesgo la seguridad del Estado y por tal razón se ha hecho evidente que "el desarrollo tecnológico exige la renovación de los medios y los métodos para la recolección de datos, así como de técnicas para la operación de equipos"[134].

Fue esta nueva realidad informática, la que llevó a la alianza estrecha entre agencias, universidades e industria, la cual ha sido redituable en materia de seguridad, pero mermó la confianza en los usuario de Internet, al dar a conocer que empresas como Google, Apple, Facebook y Microsoft habían proporcionado información de sus usuarios a la NSA[135], lo cual creó una masa crítica que demanda mecanismos de autoregulación de las agencias de Inteligencia y de los vínculos públicos- privados.

El caso de Wikileaks probó que existen actividades de espionaje realizados por las distintas embajadas estadounidenses, y si bien es cierto que ésta ha sido una

---

[133]Véase Eriksson Johan y Giacomello Giampiero, "Information Revolution, Security, and International Relations; (IR) relevant Theory?" *International Political Science Review*, *Op.cit*, pp. 221-244.
[134]Alberto Mendes Cardoso, *El papel de la actividad de inteligencia en el inicio de una nueva era*, en "Los servicios de inteligencia en el nuevo siglo"*, op.cit.,* p. 21.
[135]Glenn Greenwald y Ewen MacAskil, *NSA Prism program taps in to user data of Apple, Google and others*, [en línea], The Guardian, 7 de junio 2013, Dirección URL: http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data, [Consultado el 20 de marzo de 2014].

práctica antigua[136], la trascendencia de este fenómeno consistió en que dio a conocer información clasificada. Es decir, publicó información reservada que podría traer posibles riesgos y tanto al Estado, a las investigaciones, o a las víctimas. Adicionalmente, permitió observar que los cables diplomáticos son una herramienta para obtener información confidencial o reservada, pero también operan como un medio para instruir a los diplomáticos sobre cómo abordar las relaciones con gobiernos extranjeros, organizaciones internacionales y otros públicos[137]. Por ello, se tradujo en el cuestionamiento a la política exterior norteamericana, pero también a los vínculos entre diplomacia, agencias de inteligencia, tecnología informática, empresas privadas, universidades y gobierno.

Dichos cables contenían información sobre temas sensibles como: corrupción, abusos a los derechos humanos, negociaciones secretas, opiniones personales y espionaje de personajes y líderes mundiales importantes. En virtud de ello, es importante realizar un análisis de las consecuencias internas para el gobierno norteamericano, así como sus efectos en las relaciones internacionales.

A nivel interno, la filtración de estos cables evidenció las debilidades en las políticas de seguridad cibernética norteamericana, lo que llevó tanto al gobierno como a las agencias de inteligencia a realizar una revisión de los sistemas internos de seguridad y a mejorar los protocolos de seguridad. Además permitió conocer el papel de las agencias de inteligencia en el manejo de información, la gran cantidad de presupuesto destinado a este objetivo y la política de espionaje implementada por el gobierno norteamericano.

---

[136]Al ser "el método para compartir el análisis de la situación en un país, y su envió sirve para componer un refrito que pueda leer el ministro para obtener la información que necesita" Borja Bengareche, Wikileaks confidencial, España, Ed. Anaya Mutimedia, 2011, p. 140.

[137]Cita textual en ingles; *"the diplomatic cables, a tool used by many governments, provides an official channel for U.S. diplomats abroad to report back to Washington and for Washington to instruct diplomats on how to approach relationships with foreign governments, the public overseas, international organizations and many other audiences".* Samuel Witten, The *Effects of Wikileaks on Those Who Work at the State Department*, [en línea], Opinion Juris, 18 de diciembre 2010, Dirección URL:http://opiniojuris.org/2010/12/18/the-effects-of-wikileaks-on-those-who-work-at-the-state-department/, [Consultado el 4 de marzo de 2014].

Finalmente, también generó alertas sobre la manera en que estas agencias de inteligencia manejaban la información, sobre la falta de supervisión de su labor y su falta de rendición de cuentas. La principal preocupación es que las acciones de espionaje, escuchas telefónicas o de correos en la red representaban un atentado a los derechos de los ciudadanos y a la libertad de expresión porque implicaba una intromisión del Estado en la vida personal.

3.1 Agencia de Seguridad Nacional (NSA) y Agencia Central de Inteligencia (CIA)

Para entender mejor las consecuencias que trajo consigo la filtración de información clasificada es preciso hacer un breve recuento de cómo funcionan las principales agencias de inteligencia de los Estados Unidos: la Agencia de Seguridad Nacional (NSA, siglas en ingles) y la Agencia Central de Inteligencia (CIA, siglas en ingles), ambas encargadas de recopilar y analizar información de gobiernos, corporaciones o individuos.

Es preciso también aclarar que las actividades de inteligencia norteamericanas son en primer lugar encabezadas por el Presidente, pero también participan los comités, los grupos de trabajo del Congreso y las propias agencias que en su conjunto están encargadas de la seguridad nacional y comúnmente se les denominada "Comunidad de Inteligencia"[138]. Es decir, esta Comunidad junto con el Poder Ejecutivo y el Poder Legislativo son encargadas del control de la seguridad nacional

[138] La Comunidad de Inteligencia esta integrada por 14 oficinas del gobierno de los Estados Unidos dentro de ellas esta; Office of the National Intelligence Director; Central Intelligence Agency (CIA); National Security Agency (NSA); Defense Intelligence Agency (DIA); National Geospatial-Intelligence Agency (NGA); National Reconnaissance Office (NRO);Department of Defense; Intelligence elements of the Army, the Navy, the Air Force, the Marine Corps; FBI; Department of Energy; Bureau of Intelligence and Research of the Department of State; Office of Intelligence and Analysis of the Department of the Treasury; DHS, Office of Intelligence of the Coast Guard Véase: s/a, La Comunidad de Inteligencia Norteaméricana, [en línea], Intel Page, Dirección URL: http://www.intelpage.info/web/exterior/estadosunidos.htm, [Consultado el 10 de marzo de 2014].

La Agencia de Seguridad Nacional (NSA)[139] tiene como objetivo asegurar la información. Opera bajo la jurisdicción del Departamento de Defensa, y tiene la obligación de dar informes al Director de Inteligencia Nacional. El Director de la Agencia de Seguridad Nacional es nombrado por el Departamento de Defensa y ratificado por el Presidente[140], actúa como Gerente Nacional de Sistemas de Seguridad Nacional ante el Secretario de Defensa y el Director de Inteligencia Nacional[141] y se desempeña como Jefe del Servicio Central de Seguridad (CSS, siglas en ingles)[142] y Comandante del CYBERCOM.

Sus principales tareas son la vigilancia, decodificación, traducción y análisis de la información, la obtención de datos de inteligencia y contrainteligencia extranjera. Tiene dos misiones principales, la primera es la Señal de Inteligencia (SIGINT, siglas en ingles) que permiten la recopilación de información que los adversarios pretenden mantener en secreto en el exterior, la cual es obtenida por medio de sistemas electrónicos extranjeros. La segunda misión es el Aseguramiento de Información (IA, siglas en ingles) que permite mantener resguardada la información de seguridad nacional prohibiendo el acceso no autorizado a los sistemas de información, para de esta manera evitar el robo de información. La conjunción de estas dos misiones permite establecer la denominada Red de Guerra (*Network Warfare*).

---

[139]Fundada el 4 de noviembre de 1952 bajo la administración Harry Truman, como una medida que permitía al Departamento de Defensa conseguir apoyo en operaciones militares de criptología para de esta manera poder descifrar los códigos japoneses y alemanes durante la Segunda Guerra Mundial.

[140]Según la Orden Ejecutiva 12333 firmada el 4 de diciembre de 1981, uno de los principales marcos jurídicos de la NSA, que da la autoridad a la NSA de recolectar, analizar y retener información de señales de inteligencia extranjeras alrededor del mundo.

[141] Nacional Security Agency, *Mission*, Nacional Security Agency, [en línea], Estados Unidos, Dirección URL:http://www.nsa.gov/about/mission/index.shtml, [Consultado el 5 de marzo de 2014].

[142]CSS funge como enlace entre la NSA y las fuerzas armadas (armada, ejército, fuerza aérea, marina y guardia costera). Establecida en 1972, está bajo el cargo del Director de la NSA. Véase: Nacional Security Agency, *Frequently Asked Questions About NSA,* [en línea], Estados Unidos, Dirección URL: http://www.nsa.gov/about/faqs/about_nsa.shtml#about1, [Consultado el 10 de marzo de 2014].

Un punto muy importante a destacar es el enorme poder de la NSA frente a la CIA[143], ya que cuenta con mayores atribuciones para realizar actividades fuera de lo establecido, porque sus actividades no son delineadas ni aprobadas por el Congreso, y por tal razón no es objeto de una supervisión, aunque sus actividades incluyen todas las actividades de vigilancia pasiva incluyendo las infiltraciones[144]. Su labor sólo es supervisada por el Comité Especial de Seguridad Nacional integrado por el Departamento de Defensa, Secretaría de Estado y el Presidente. Ello explicara el por qué esta agencia tiene mayores posibilidades de realizar actividades fuera de lo establecido, frente al resto de las agencias de inteligencia. Sin embargo, también debemos mencionar que esta agencia no está autorizada para llevar a cabo recolección de información a través de fuentes humanas como sucede en el caso de la Agencia Central de Inteligencia, por lo cual el ciberespacio ha sido una de sus principales terrenos de acción.

Por otra parte, la Agencia Central de Inteligencia (CIA)[145] tiene facultad de realizar misiones humanas en el exterior y en diversas áreas como drogas, terrorismo, tráfico de armas, etc. Opera bajo el principio de recopilar información, analizar, evaluar y difundir información de inteligencia extranjera para ayudar a los tomadores de decisiones a resolver controversias en materia de seguridad

---

[143]Cita textual en ingles: *"The specific duties of NSA were neither delineated by nor approved by Congress. NSA is subject to no congressional oversight, but their duties include all passive intelligence gathering, including infiltration"* Nelson McAvoy, *Coded Messages: How the CIA and NSA Hoodwink Congress and the People*, Estados Unidos, Ed. Algora Publishing, 2010, p.7

[144] Cita textual en ingles: *"The specific duties of NSA were neither delineated by nor approved by Congress. NSA is subject to no congressional oversight, but their duties include all passive intelligence gathering, including infiltration"* Nelson McAvoy, *Coded Messages: How the CIA and NSA Hoodwink Congress and the People*, Estados Unidos, Ed. Algora Publishing, 2010, p.7

[145]Fue creada el 18 de diciembre de 1947 bajo el mandato presidencial de Harry S. Trumman en sustitución de la Oficina de Servicios Estratégicos (OSS) que funcionó durante la Primera Guerra Mundial. Quedó bajo la responsabilidad del Director de la CIA también la función de Director de Inteligencia Central, es decir que fungía como cabeza de la Comunidad de Inteligencia de los Estados Unidos. Véase: *About CIA*, [en línea], Center of Intelligence Agency, Dirección URL:https://www.cia.gov/about-cia, [Consultado el 11 de marzo de 2014].

nacional[146]. Es por estas razones que tiene fuertes vínculos con los grupos diplomáticos y el sector gubernamental.

La agencia para cubrir sus funciones se organiza en cuatro grupos[147,] los cuales llevan a cabo el denominado "ciclo de inteligencia" que consiste en la recopilación, análisis y difusión de informaciones entre los altos funcionarios del gobierno de los Estados Unidos. El Director de la CIA es nombrado por el Presidente y debe ser ratificado por parte del Senado, es la cabeza de la agencia y está encargado de manejar el presupuesto, las operaciones y al personal.[148] La CIA se rige bajo los estatutos de la *National Security Act* (Ley de Seguridad Nacional)[149]. Sin embargo, esta acta ha sufrido algunas modificaciones a lo largo de los años. En esta investigación es importante hacer mención a las reformas de la Comisión Rockefeller[150], Ley de Supervisión de Inteligencia[151] y al Acta de la Reforma de

---

[146]*Ibidem.* Dirección URL:https://www.cia.gov/about-cia

[147]El Servicio Nacional Clandestino (recopilación de información extranjera de manera clandestina proporcionado por fuentes humanas), la Dirección de Inteligencia (analiza la información para producir informes), la Dirección de Ciencia y Tecnología (con la información colabora con la generación de innovaciones científicas y técnicas) y la Dirección de Apoyo (proporciona apoyo en distintas áreas instalaciones, logística, información, etc. Véase Who we are, [en línea], Central Intelligence Agency, 5 de abril de 2007, Dirección URL: https://www.cia.gov/about-cia/todays-cia/who-we-are, [Consultado el 11 de marzo de 2014].

[148]Leadership, Center of Intelligence Agency, [en línea], Dirección URL: https://www.cia.gov/mobile/about-cia/leadership/index.html, [Consultado el 11 de marzo de 2014].

[149]Creada el 26 de julio de 1947 en donde se establece el marco jurídico de esta agencia. Véase U.S Department of State, National Security Act of 1947, [en línea], Dirección URL:https://history.state.gov/milestones/1945-1952/national-security-act, [Consultado el 11 de marzo de 2014].

[150]En 1974 a cargo del vicepresidente Nelson Rockefeller. Que tuvo por objeto "investigar supuestas actividades ilegales en la CIA, (…) espionaje ilegal contra estadounidense, intercepción ilegal de correo, violencia física, robo, proyectos ilegales"[150] tras el término de la investigación se estableció la obligación por parte de la CIA de presentar auditorias para la evaluación de sus actividades. Véase Tesis Ortega Zacarías Roberto, La importancia geopolítica de los servicios de inteligencia civiles como instrumento de política exterior: el caso del Centro de Investigación y Seguridad Nacional (2000-2012), UNAM, Facultad de Estudios Superiores Aragón, enero 2013, p. 22.

Inteligencia y Prevención del Terrorismo en 2004[152] que brindaron la posibilidad a distintas instancias gubernamentales de mantener un mayor control sobre las actividades realizadas por esta agencia, al obligarla a rendir cuentas, presentar auditorias y supervisión de sus actividades. Es decir, la CIA adquirió mayores regulaciones de sus actividades frente a la NSA.

El verdadero problema de las agencias de inteligencia de los Estados Unidos radica en que sus actividades son secretas, lo cual abre la posibilidad de abusos potenciales que no tomen en cuenta los derechos civiles de los ciudadanos y la posibilidad de que su actuación rompa la relación de confianza entre la comunidad de inteligencia, los encargados de establecer políticas y el público en general[153]. Esta última posibilidad existe porque las agencias de inteligencia cuentan con autoridad discrecional para cumplir con sus funciones y tiene autonomía para

---

[151]En 1980 estableció el Comité Selecto de Inteligencia del Senado (SSCI, siglas en ingles) y el Comité Selecto Permanente de Inteligencia (HPSCI) encargados de la supervisión de las actividades de las agencias de inteligencia. Con la Comisión Murphy en 1992 realizada por Martha Wagner Murphy trajo como consecuencia que "todos los documentos de la Agencia (…) tenían que ser informados a los diferentes organismos supervisores de la misma" que llevó a reafirmar la obligación de la agencia de rendir cuentas de las actividades que realizaba. Véase: Tesis Ortega Zacarías Roberto, *La importancia geopolítica de los servicios de inteligencia civiles como instrumento de política exterior: el caso del Centro de Investigación y Seguridad Nacional (2000-2012), op.cit*., p. 23.

[152]El gobierno de George W. Bush creó la Acta de la Reforma de Inteligencia y Prevención del Terrorismo en 2004, creando la figura del Director Nacional de Inteligencia y por el otro el Director de la Agencia Central de Inteligencia que se convierte en Director Nacional de Inteligencia.

[153]Cita textual en ingles: *"While secrecy is considered indispensable in intelligence, it also contains in it the potencial for abuse, lending weight to what has become one of the most widely used images of intelligence services as a 'rogue elephant', out of control and trampling civil rights and liberties, undermining the relationship of trust that should exist between the intelligence community and policy-makers as well as the general public".* Hans Born y Marina Caparini, Democratic Control of Intelligence Service: Containing Rogue Elephants, Gran Bretaña, Ed. Ashgate Publishing Company, 2007, p. 18, [en línea], Dirección URL: http://books.google.com.mx/books?id=FeGhAgAAQBAJ&pg=PA18&lpg=PA18&dq=intelligence+agencies+out+of+control&source=bl&ots=_jOMsbAOiX&sig=7ofbt8IGXVlXx1_BmrC1e8YVzU8&hl=es&sa=X&ei=lUUGVIWME4y-ggSWtICwCg&ved=0CFQQ6AEwBDgK#v=onepage&q=intelligence%20agencies%20out%20of%20control&f=false, [Consultado el 13 de abril de 2014].

evitar la interferencia política en asuntos de inteligencia y así evitar responder ante intereses particulares[154].

Por otra parte, el hecho de que las agencias cuenten con autonomía para definir los procedimientos a utilizar para obtener la información, incluyendo la de ciudadanos norteamericanos[155], incluso sin consultarlos con el Presidente es un tema controvertido, porque significa que en la práctica es una falacia la custodia de las autoridades sobre los servicios de inteligencia.

Finalmente, la vigilancia de los ciudadanos norteamericanos, afecta el respeto a su privacidad en Internet y los estándares de encriptación de la información privada, por lo cual algunos grupos demandan establecer un balance entre la seguridad y las libertades democráticas, para evitar que las agencias de inteligencia interfieran con derechos civiles en su búsqueda de asegurar la nación, obteniendo información de personas que incluso no están acusadas de ningún delito.

3.2 Protocolos de seguridad de información en las Agencias de Inteligencia

Tras la filtración de los cables del Departamento de Estado de los Estados Unidos, el gobierno incrementó y modificó los protocolos de seguridad de la información considerada como reservada o clasificada, para evitar una nueva filtración de información. Los lineamientos fueron aplicados tanto en agentes externos, como en el personal de las agencias de inteligencia con acceso a esta información.

---

[154]Cita textual en ingles: *"[…] intelligence practitioners are granted a certain (and often significant) amount of discretionary authority in order to fulfil their functions. This constitutes a sphere of autonomy which is considered necessary to avoid politicization of intelligence and the production of 'intelligence to please'"* Hans Born y Marina Caparini, Democratic Control of Intelligence Service: Containing Rogue Elephants, *op.cit*, p. 18.

[155]Cita textual en ingles: *"The NSA is not supposed to spy on American citizens, but it "incidentally" collects vast amounts of data on them anyway".* T.C. Sottek, The NSA is out of control and must be stopped, The Verger, 12 de diciembre 2013, [en línea], Dirección URL:http://www.theverge.com/2013/12/12/5200142/end-the-nsa-nightmare, [Consultado el 15 de abril de 2014].

Borja Bengareche define el proceso en los siguientes términos "la Administración de E.E.U.U. tuvo dos reflejos internos inmediatamente: restringir los procesos de desclasificación de los documentos (…) y revisar la seguridad en la red de intercambio de información entre las agencias conocidas como *SIPRNet*"[156]. Como parte de este proceso se incluyó la utilización de puertos USB y el monitoreo de todos los equipos con acceso a la red, como medidas para evitar nuevas fugas de información.

Asimismo, el Departamento de Defensa estableció otros cambios en los protocolos de seguridad en materia de manejo de la información entre los que destacan "cada usuario autorizado a utilizar la red deberá insertar una tarjeta que permitiera su total identificación por el sistema, y reconociera la actividad realizada en la red secreta. Esta llave identificativa, denominada *Public Key Infrastructure* o PKI (siglas en ingles)[157], debería estar repartida a todos los usuarios antes de finales de 2012"[158]. Esto significaba que se restringía el acceso a la información clasificada a personal confiable, el cual sería monitoreado y para realizar cambios en al material clasificado requeriría autorización.

Por otra parte, como se mencionó en el primer capítulo, previo a la filtración de Wikileaks, el Departamento de Estado utilizaba como programa para comunicarse con el resto de sus embajadas y sedes en el extranjero el sistema *SIPRENet,* el cual fue utilizado para tener acceso a la información confidencial filtrada, por lo

---

[156] Borja Bengareche, *Wikileaks confidencia*, España, Ed. Anaya Mutimedia, 2011, p. 153.
[157] PKI permite intercambiar información en redes públicas no seguras a través del uso de claves criptográficas, las cuales necesitan de un certificado digital por parte de una autoridad certificada. Véase PKI: http://searchsecurity.techtarget.com/definition/PKI, [Consultado el 21 de marzo de 2014].
[158] Borja Bengareche, Wikileaks confidencia, España, Ed. Anaya Mutimedia, 2011, p. 154.

cual el Departamento de Estado desconectó de su red gubernamental este sistema, como una medida para asegurar la información[159].

Esto nos lleva a concluir que se realizaron algunos cambios en los protocolos de seguridad del personal con acceso a información clasificada, restringiendo el personal con acceso y estableciendo estrategias de monitoreo. Sin embargo, las medidas correctivas conocidas fueron mínimas, frente a los escándalos, pero se desconoce cuáles fueron los cambios de fondo en estos protocolos por ser material clasificado.

3.3 Presupuesto Federal destinado a las Agencias de Inteligencia

Después de los atentados terroristas del 11 de septiembre de 2001 el gobierno de los Estados Unidos y el Congreso decidieron incrementar el presupuesto destinado a las agencias de inteligencia para de esta manera evitar nuevos atentados. Las agencias de inteligencia deben ahora realizar una solicitud de presupuesto, la cual está condicionada en primer lugar por el representante de las agencias patrocinadoras, quien deberá remitirlo a la Oficina de Manejo de Presupuesto de la Casa Blanca. Y una vez enviado a esta oficina es revisado por el Congreso, por los Comités de Inteligencia de ambas Cámaras quienes lo discuten y analizan[160].

---

[159]Cita textual en ingles: "*in response to the leaks, the State Department disconnected itself from Defense's SIPRNet, thereby securing its information from potential leaks by non-State Department employees and removing the agency from at least part of its information-sharing commitment with Defense".* Mark Fenster, "Disclosure's Effects: WikiLeaks and Transparency", [en línea], Estados Unidos, *Revista Iowa Law Review,* Universidad de Iowa, Vol. 97:753, 2012, p. 797, Dirección URL:http://www.uiowa.edu/~ilr/issues/ILR_97-3_Fenster.pdf, [Consultado el 12 de marzo de 2014].

[160]*Cita textual en ingles: "the request of the intelligence agencies are first coordinated by representatives of sponsoring agencies before being submitted to OMB for careful review (…) Once the president's budget is submitted to Congress, the portion for the intelligence agencies is segregated from the rest and discussed by members of the House and Senate Intelligence Committees".* Banks William C., *National Security Law and the Power of the Purse*, Estados Unidos, Ed. Oxford University Press, 1994, p 52.

El procedimiento seguido muestra que para incrementar el presupuesto en materia de inteligencia requiere primero establecer acuerdos y cabildeos entre las agencias, con el Ejecutivo y el Congreso, por lo tanto no es una decisión unilateral sino colegiada.

Como podemos observar en la Tabla 2 el presupuesto destinado a la inteligencia se ha incrementado durante los últimos años[161].

[161] Cita textual en ingles: *"the U.S. intelligence budget (excluding the Military Intelligence Program) in fiscal year 2012 was $53.9 billion, (…) This figure is up from $53.1 billion in 2010, $49.8 billion in 2009, $47.5 billion in 2008, $ 43.5 billion in 2007, and $40.9 billion in 2006."* International Business Publications, Inc, *US Central Intelligence Agency (CIA) Handbook-Strategic Information*, [en línea], Estados Unidos, Ed. International Business Publications, Inc, 2013, Pp. 18-19, Dirección URL: http://books.google.com.mx/books?id=4VubAAAAQBAJ&pg=PA18&lpg=PA18&dq=%E2%80%9Cthe+U.S.+intelligence+budget+in+fiscal+year+2012+was+$53.9+billion,&source=bl&ots=-I8TVWdsts&sig=v0On3Ai_tPi4HwLOXzZgazzO-2I&hl=es&sa=X&ei=XVZyU_uZN-TL8QH5jIGYDw&ved=0CIoBEOgBMAg#v=onepage&q=%E2%80%9Cthe%20U.S.%20intelligence%20budget%20in%20fiscal%20year%202012%20was%20%2453.9%20billion%2C&f=false, [Consultado el 15 de marzo de 2014].

Tabla 2 Presupuesto de Inteligencia 2006-2013

En junio de 2007, el Director de Inteligencia Nacional dio a conocer la revisión del presupuesto del año fiscal 2014 para el Programa de Inteligencia Nacional (NIP, siglas en ingles) fue de $52.2 billones de dólares, incluyendo el presupuesto requerido para las operaciones de contingencia en el extranjero de 2014. El Departamento de Defensa también dio a conocer el presupuesto del año fiscal 2014 para el Programa de Inteligencia Militar (MIP, siglas en ingles) que de fue $18.6 billones de dólares.

Intelligence Budget Data

On June 27, 2013, the Director of National Intelligence disclosed that the revised FY 2014 budget request for the National Intelligence Program (NIP) was $52.2 billion, including the budget request for FY 2014 Overseas Contingency Operations. The Department of Defense disclosed that the revised Military Intelligence Program (MIP) budget request for FY 2014 was $18.6 billion.

FISCAL YEAR	NIP BUDGET	MIP BUDGET	TOTAL
2013	52.7 billion (reduced by sequester to 49.0 billion)	19.2 billion (reduced by sequester to 18.6 billion	71.9 billion (reduced by sequester to 67.6 billion)
2012	53.9 billion	21.5 billion	75.4 billion
2011	54.6 billion	24 billion	78.6 billion
2010	53.1 billion	27 billion	80.1 billion
2009	49.8 billion	26.4 billion	76.2 billion
2008	47.5 billion	22.9 billion	70.4 billion
2007	43.5 billion	20 billion	63.5 billion
2006	40.9 billion		

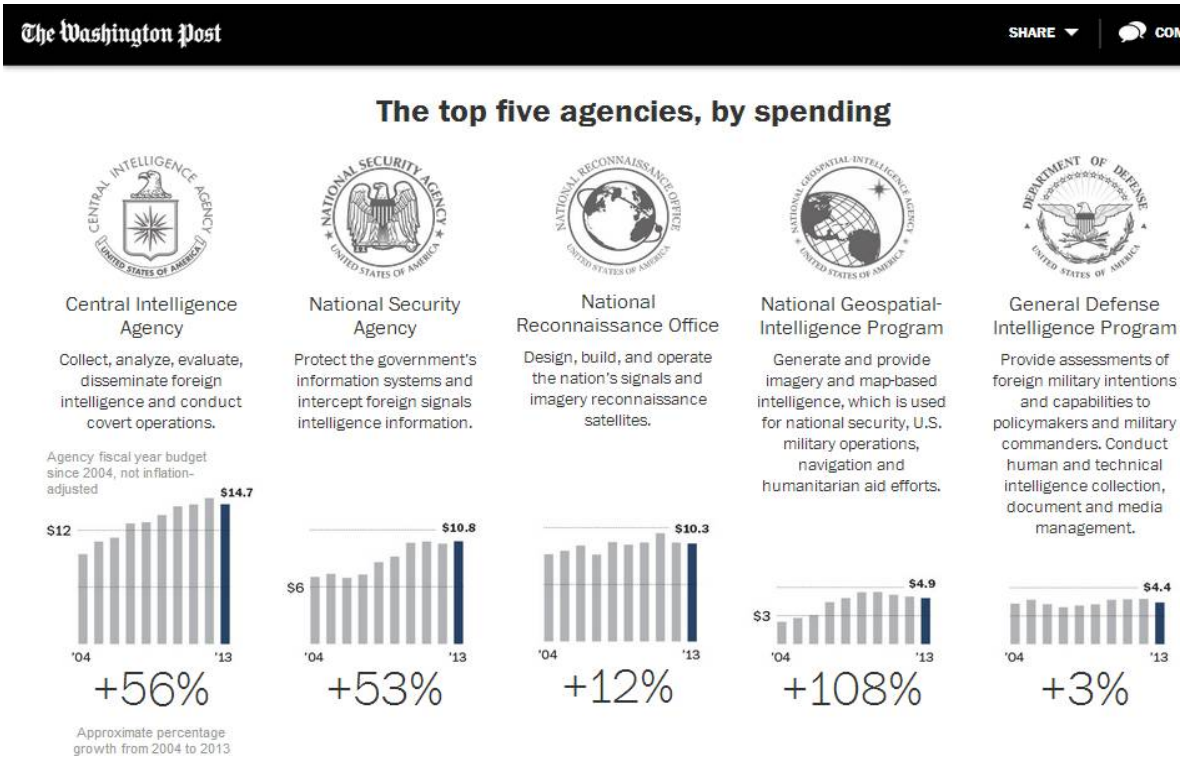
FAS, *Intelligence Budget Data*, Estados Unidos, [en línea], Dirección URL: http://www.fas.org/irp/budget/index.html?PHPSESSID=70809e6b347db7b2122df1ef24d743e0, [Consultado el 16 de marzo de 2014].

Además, esta tabla nos demuestra que el presupuesto destinado a inteligencia es casi lo doble que el presupuesto destinado a los Programas Militares, lo cual muestra que durante las últimas administraciones del gobierno de los Estados Unidos las actividades de inteligencia se volvieron muy importantes.

También es necesario tener en cuenta que el Programa Nacional de Inteligencia recibe 80% del total del presupuesto de inteligencia, incluyendo las actividades de inteligencia de la Oficina de Reconocimiento Oficial a las que se destinan $8 billones de dólares, misma cantidad que recibe la NSA, mientras la CIA recibe $6 billones de dólares. La Agencia Nacional de Inteligencia-Geoespacial recibe

$ 3 billones y el FBI solo $1.5 billones[162]. Todo ello demuestra que en el Programa Nacional de Inteligencia (NIP, siglas en ingles) se establecen los montos que recibirán las principales agencias de inteligencia de los Estados Unidos, y por tal razón tiene gran importancia para esta comunidad de los Estados Unidos.

Tabla 3 Top 5 de las agencias de inteligencia según sus gastos



Washington Post, *The Black Budget,* [en línea], Estados Unidos, Washington Post, Dirección URL: http://www.washingtonpost.com/wp-srv/special/national/black-budget/,[Consultado el 18 de marzo de 2014].

[162]Cita textual en ingles: "*the National Intelligence Program (NIP) receives about 80 percent of the total intelligence budget. It includes the intelligence activities of the National Reconnaissance Office ($8 billions); the National Security Agency ($8 billions); the National Geospatial-Intelligence Agency ($3 billions); the Central Intelligence Agency ($6 billions); the FBI ($1.5 billion); the Department of Homeland Security ($12 million); the State Department's Bureau of Intelligence and Research ($60 millions); and the Treasury Department ($60 million).*" Tim Shorrock, *Spies for Hire: The Secret World of Intelligence Outsourcing, op. cit,* p. 20.

Como podemos ver con la tabla 2 la *Central Intelligence Agency* (CIA) tuvo un incremento del 56% de su presupuesto en 2013 ($14.7 billones), ya que en 2004 recibió $12 billones de dólares. Esto significa que se utiliza el 28 % del total del presupuesto para inteligencia. Por otra parte, la *National Security Agency* (NSA) incrementó su presupuesto de $6 billones de dólares en 2004 a $10.8 billones de dólares en 2013, lo cual significa un aumento del 53% en el presupuesto destinado a esta agencia.

Sin embargo, debemos tener en cuenta que del monto del presupuesto federal para inteligencia el 70% se destina a contratistas privados. Se estima que de los $80 billones de dólares, $56 billones de dólares se destinaron al sector privado[163]. Esto significa que se han incrementado los costos por la subcontratación privada, así como las dificultades para el resguardo de la información, como veremos en el siguiente subtitulo.

De todo el presupuesto que reciben las agencias de inteligencia, una gran parte se destina al pago de la nómina, por lo que se han registrado diversas propuesta de recortes de personal. Una de ellas se dio en 2013 cuando la NSA presentó una iniciativa que impliacaba el despido de 21,575 pesonas. Mientras que la CIA planteaba en su propuesta reducir el total de su personal a los 22,206 personas que laboran actualmente[164].

Sin embargo, el problema es que los recortes han ido acompañados del incremento en la subcontratación de empresas privadas, buscando con este

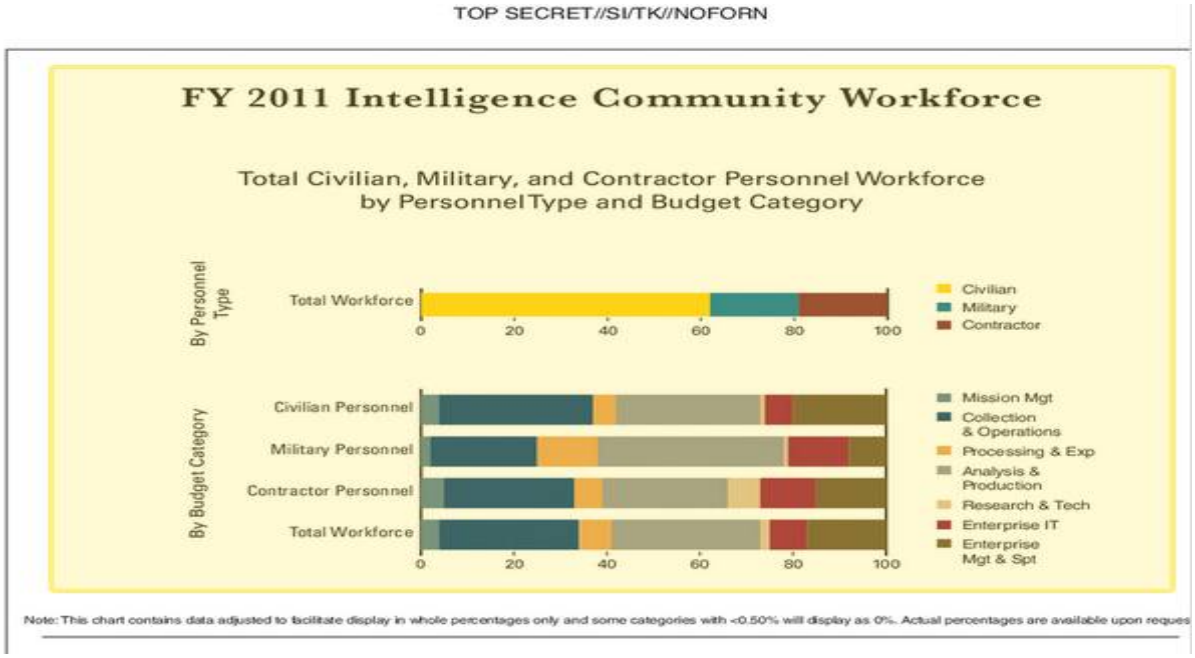
---

[163] Tim Shorrock, *Put the Spies back under one roof*, [en línea], Estados Unidos, The New York Times, The Opinion pages, 17 de junio 2013, Dirección URL:http://www.nytimes.com/2013/06/18/opinion/put-the-spies-back-under-one-roof.html?ref=centralintelligenceagency, [Consultado el 18 de marzo de 2014].

[164] *Cita textual en inglés:"the NSA requested $10.45 bn, an increase of 3% on last year. The agency plans to reduce headcourt by 75 in 2013, which would leave 21,575 personnel. Bye comparison, the CIA has 22,206 personnel and is requesting 14.7bn down 4% on last year"* Ewen MacAskil; Jonathan Watts, *US intelligence spending has doubled since 9/11, top secret budget reveals,* [en línea], The Guardian, 29 de agosto 2013, Dirección URL: http://www.theguardian.com/world/2013/aug/29/us-intelligence-spending-double-9-11-secret-budget, [Consultado el 19 de marzo de 2014].

mecanismo reducir su gasto corriente pero sin disminuir su labor. Sin embargo, esta estrategia resulta contraproducente a largo plazo, porque es más costosa para el gobierno.

Tabla 4 Fuerza de trabajo de la Comunidad de Inteligencia 2011



s/a, *FY 2013 Congressional Budget Justification,* [en línea], Estados Unidos, Washington Post, Febrero 2012, Dirección URL: http://apps.washingtonpost.com/g/page/national/inside-the-2013-us-intelligence-black-budget/420/#document/p1/a117329, [Consultado el 19 de marzo de 2014].

La mayoría de los datos aquí presentados tienen como fuente el periódico Washington Post y fueron proporcionados por Edward Snowden, ex contratista de inteligencia de la NSA, quien dio a conocer información sobre "*black budget" o* presupuesto negro de las agencias de inteligencia. La información generó polémica porque permitió conocer los altos montos destinados a inteligencia y las dificultades para lograr que funcionen de manera más eficiente.

3.4 Supervisión de las Agencias por parte del Congreso

La supervisión de las actividades de inteligencia en los Estados Unidos está regida bajo el Acta de Autorización de Inteligencia[165] la cual refuerza el poder de supervisión por parte de los comités tanto de la Cámara Alta como de la Cámara Baja. La Cámara Baja integra la Comisión Especial Permanente de Inteligencia (HPSCI, siglas en ingles) compuesta por 22 miembros, los cuales incluyen al menos a un miembro de los Servicios Armados, del Poder Judicial y de los Comités de Asuntos Exteriores. Por otra parte, la Cámara Alta a su vez tiene a la Comisión Especial de Inteligencia del Senado (SSCI) compuesta por 15 senadores, de los cuales 8 pertenecen al partido mayoritario. También está integrada por un miembro de las Fuerzas Armada, de Relaciones Exteriores y del Poder Judicial[166], quienes están encargado de supervisar las actividades, para de esta manera mantener un balance en el sistema de inteligencia y estar enterados de todas las actividades que se realizan.

Está estipulado que tanto el Presidente de los Estados Unidos, como los miembros del Comité de inteligencia del Poder Legislativo y las agencias deben mantenerse en constante coordinación sobre las actividades que realizan en pro de la protección del Estado. El Estatuto Básico estipula que el Presidente debe asegurarse de que el Comité de Inteligencia del Congreso esté informado de las actividades de inteligencia que estén realizando las agencias, incluyendo las

---

[165] Esta Acta se firmó el 20 de octubre de 1998 Véase George Bush Intelligence Center, [en línea], Estados Unidos, CIA, Dirección URL:https://www.cia.gov/about-cia/todays-cia/george-bush-center-for-intelligence, [Consultado el 21 de marzo de 2014].

[166] Eric Rosenbach, *Congressional Oversight of the Intelligence Community*, [en línea], Belfer Center for Science and International Affairs, Harvard Kennedy School, julio 2009, Dirección URL:http://belfercenter.ksg.harvard.edu/publication/19146/congressional_oversight_of_the_intelligence_community.html, [Consultado el 21 de marzo de 2014].

actividades de previsión[167]. Sin embargo, a pesar de lo estipulado, la filtración de información por parte del ex contratista de la NSA Edward Snowden mostró que las agencias de inteligencia, particularmente la NSA recolectan escuchas telefónicas no solamente del extranjero sino también de ciudadanos norteamericanos sin el consentimiento de los Comités de Inteligencia del Congreso, amparándose en las atribuciones adquiridas a partir de 2008. Es decir, tanto el Acta Patriota que ya revisamos anteriormente, como la FISA contribuyeron a que las agencias realizaran actividad de espionaje hacia otros sectores no autorizados directamente[168].

La filtración de información clasificada generó cuestionamientos hacia los actores que supuestamente debían supervisar las labores de inteligencia. Se argumentó que no han fungido como guardines por sus posturas acríticas hacia la Comunidad de Inteligencia y que los miembros del Comité de Inteligencia del Congreso tienen pocos incentivos para desarrollar experiencia en asuntos de inteligencia debido a sus constantes cambios de actividades[169]. Finalmente, que no están en posibilidades de supervisar el empleo del secreto de Estado, porque aun cuando

---

[167]Cita textual en ingles: *"the basic statute requires that the "President shall ensure that the intelligence committees are kept fully and currently informed of the intelligence activities of the United States, including any significant anticipated intelligence activity as required by this title*". Elaine Halchin; Frederick M. Kaiser, *Congressional Oversight of Intelligence: Current Structure and Alternatives*, [en línea], Congressional Research Service, 14 mayo 2012, p.33, Dirección URL: http://www.fas.org/sgp/crs/intel/RL32525.pdf, [Consultado el 21 de marzo de 2014].

[168]Cita textual en ingles: *"the NSA broke privacy rules or overstepped its legal authority thousands of times each year since Congress granted it broad new power in 2008" s/a, Inhofe wants to investigate NSA, following new report about surveillance,* [en línea], Fox News, 17 de agosto 2013, Dirección URL: http://www.foxnews.com/politics/2013/08/17/inhofe-calls-for-hill-investigations-after-new-report-about-nsa-surveliance/#ixzz2cGWCrhe0, [Consultado el 22 de marzo de 2014].

[169]Cita textual en ingles*: "the overseers themselves, a great many of whom, Loch Johnson has argued, have acted not as watchful "guardians" of the public trust, but rather as uncritical "cheerleaders" for the intelligence community. Another explanation draw attention to the high turnover and large memberships of the intelligence oversight committees, which according to two recent congressional reports, gives members little chance on incentive to develop expertise in intelligence affairs"* Rahul Sagal, *Secrets and leaks: the dilemma of state secrecy*, Estados Unidos, Ed. Princeton University Press, 2013, p. 81.

tiene la fuerza para desafiar al presidente, no pueden obtener fácilmente la información necesaria para llevar a cabo una verdadera supervisión[170].

Por otra parte, la filtración generó una reflexión al respecto. El senador Jim Inhofe, de Oklahoma, consideró que los abusos de la NSA son preocupantes ya que significan que la administración de Obama ha abusado de su autoridad en materia de espionaje.*[171]*

En contraste, el Poder Ejecutivo de los Estados Unidos argumentó que los miembros del Congreso sabían de las extensivas actividades de escaneo telefónico y espionaje de correos electrónicos realizados por la Agencia de Seguridad Nacional*[172]*, pero no realizaron ninguna acción para detener o sancionar estas actividades.

La crítica fundamental en la opinión pública es que la supervisión por parte del Congreso en materia de inteligencia ha sido disfuncional*[173]*.

Los miembros del propio Comité de Inteligencia, como la Senadora Dianne Feinstein[174], Presidenta del Comité de Inteligencia del Senado[175], manifestó su

---

[170] Cita textual en ingles: "*Congress is not well positioned to oversee the employment of the state secrecy because ever when it has the will power to challenge the president, it cannot easily obtain the information it needs to conduct oversight"* Rahul Sagal, o*p.cit*., p. 101.

[171]Cita textual en ingles: *"the NSA violations are very concerning as it appears the Obama Administration has abused the authority granted to team by Congress". s/a,* Inhofe wants to investigate NSA, following new report about surveillance, [en línea], Fox News, 17 de agosto 2013, Dirección URL: http://www.foxnews.com/politics/2013/08/17/inhofe-calls-for-hill-investigations-after-new-report-about-nsa-survelliance/#ixzz2cGWCrhe0, [Consultado el 22 de marzo de 2014].

[172] Cita textual en ingles: "*The White House insists members of Congress knew full well about the National Security Agency's almost unabridged ability to scan phone logs and Internet chats for terrorist threats".* Tony Romm, Intelligence Oversight has some limits in Congress, [en línea], Político 10 de octubre 2013, Dirección URL: http://www.politico.com/story/2013/10/intelligence-oversight-has-some-limits-in-congress-98099.html, [Consultado el 21 de marzo de 2014].

[173] Cita textual en ingles: "*intelligence oversight by Congress is described by commentators and members of Congress alike as dysfunctional".* Denis McDonoug; Mara Rudman; Peter Rundlet, *No Mere Oversight Congressional Oversight of Intelligence is Broken*, [en línea], Center for American Progress, Junio 2006, p. 2. Dirección URL: http://www.americanprogress.org/kf/NOMEREOVERSIGHT.PDF, [Consultado el 23 de marzo de 2014].

preocupación de por qué los contratistas privados están realizando trabajos que son esencialmente responsabilidad del gobierno federal[176] y han tenido acceso a información clasificada. También señaló que las agencias de inteligencias, en particular la CIA, ha estado investigando las actividades del Comité de Inteligencia del Senado "acusó a esta organización de violar la ley federal y socavar el principio constitucional de la supervisión del Congreso de Estados Unidos. También detalló públicamente por primera vez cómo la agencia obtuvo en secreto documentos de las computadoras utilizadas por su panel para investigar un programa de interrogación controvertido"[177]. Lo cual cuál viola no solo la Cuarta Enmienda Constitucional, sino también otras leyes que prohíben las búsquedas internas y la vigilancia sin una autorización. Lo antes señalado es muestra de las confrontaciones entre el Congreso y las agencias de inteligencia.

Debemos tomar en cuenta que esta falta de vigilancia por parte de los Comités del Congreso no es un hecho novedoso, ya durante la administración de George W. Bush también se tuvo acceso a información que demostraba la existencia de una gran lista de actividades de Inteligencia que no fueron estrictamente vigiladas por el Congreso, donde se incluyen fallas en los cálculos de las armas de destrucción masiva antes de la guerra de Iraq; fallas en la denominada "fase II" de la

---

[174] Dianne Feinstein, Senadora Senior por el partido demócrata en el estado de California. Fue electa por primera vez para el Senado en 1992. A partir de 2009 durante la CXI Legislatura del Congreso fue nombrada Presidenta del Comité de Inteligencia del Senado. Adicionalmente pertenece al Comité Jurídico del Senado y al Comité de Apropiación del Senado, donde es Presidenta del Subcomité de Energía y agua. Véase: Dianne Feinstein Biography Dirección URL:http://www.feinstein.senate.gov/public/index.cfm/biography, [Consultado el 23 de marzo de 2014].

[175] El Comité de Inteligencia está encargado de autorizar y legislar sobre la CIA, al DNI, al Programa Nacional de Inteligencia Extranjera. Reciben informes por parte del Presidente, otros funcionarios y organismos. Está encargado no solo de revisar las actividades y programas de inteligencia, sino también de analizar el presupuesto destinado a las agencias.

[176] Cita textual en ingles: "[we are] *very concerned that we have government contractors doing what are essentially governmental jobs"* Tim Shorrock, *Put the Spies back under one roof*, *Op. Cit.* Dirección URL:http://www.nytimes.com/2013/06/18/opinion/put-the-spies-back-under-one-roof.html?ref=centralintelligenceagency, [Consultado el 17 de marzo de 2014].

[177]Greg Miller; Ed O'Keefe; Adam Goldman, *La CIA hackeó al Comité de Inteligencia: Dianne Feinstein*, [en línea], México, El Economista, 11 de marzo 2014, Dirección URL: http://eleconomista.com.mx/internacional/2014/03/11/cia-hackeo-comite-inteligencia-dianne-feinstein, [Consultado el 20 de marzo de 2014].

investigación del Senado concerniente a la manipulación de políticas de inteligencia; la negación a investigar reclamos de tortura y otros tratos ilegales sobre los detenidos de guerra y la imposibilidad de obtener información sobre los programas no autorizados de espionaje telefónico de la NSA[178].

A pesar de que los miembros del Comité han cambiado, el Congreso no ha tomado acciones más drásticas para lograr una mayor supervisión de las agencias. La posible confrontación con el Ejecutivo, lo polémico del tema, los diversos intereses implicados y las divisiones al interior del propio Congreso en los Comités de Inteligencia de la Cámara Baja y Alta[179], parecen ser elementos explicativos de esta dinámica que desconoce las recomendaciones de la Comisión del 11 de septiembre para reorganizar el sistema de supervisión de la comunidad de inteligencia[180].

Es preciso también mencionar que como vimos en el capítulo anterior existe un Acta Federal de Manejo de Seguridad Informática (FISA) cuyo propósito es revisar los programas establecidos por las agencias de inteligencia y debe realizar informes periódicos al Congreso sobre la situación de los programas de seguridad informática. Sin embargo, este mecanismo ha sido insuficiente para realizar

---

[178]Cita textual en ingles: *"the list of congressional oversight failures raised by these commentators typically includes: the failure of pre-Iraq war intelligence on weapons of mass destruction; the failure to conclude the so called "Phase II" of the Senate investigation regarding the political manipulation of intelligence; the refusal to investigate allegations of torture and other illegal treatment of detainees; the failure to obtain a proper understanding of (…) the NSA warrantless wiretapping program."* Denis McDonoug; Mara Rudman; Peter Rundlet, o*p.cit.*, p. 7.

[179]Cita textual en ingles: "*Congressional oversight in an unsatisfactory state…. the jurisdictional melee among scores of Congressional committees has led to conflicting and contradictory tasks and mandates for DHS."* Thomas H. Kean; Lee H. Hamilton, *Testimony, US Senate Committee on Commerce, 111 Congress, 20 de enero 2010, en Halchin Elaine y Kaiser Frederick M., Congressional Oversight of Intelligence: Current Structure and Alternatives*, [en línea], Congressional Research Service, 14 mayo 2012, p.3, Dirección URL: http://www.fas.org/sgp/crs/intel/RL32525.pdf, [Consultado el 23 de marzo de 2014].

[180]Cita textual en ingles: "*the problem is that when it comes to intelligence, Congress has been prepared to clean every house but its own. For six years it has ignored the recommendation of the Sept. 11 commission to reorganize its broken system for supervising the intelligence community".* David Ignatius, *Bipartisanship in Congress should start with intelligence oversight*, [en línea], Estados Unidos, Washington Post, 5 de diciembre 2010, Dirección URL:http://www.washingtonpost.com/wp-dyn/content/article/2010/12/03/AR2010120304304.html, [Consultado el 23 de marzo de 2014].

acciones regulatorias, ya que la Corte de la FISA, se encuentra incapacitada para aplicar sanciones a las agencias por no contar con las herramientas necesarias para verificar independientemente que la información que recibe es correcta[181].

Es decir, ni siquiera los programas creados para supervisar el funcionamiento de las programas de inteligencia están operando adecuadamente, al no contar con los medios necesarios para verificar la información que reciben y no tener la posibilidad de realizar sus propias investigaciones en materia de actividades de inteligencia, ello significa un grave problema que impide controlar a las agencias.

Existen evidencias de que hasta el momento el Congreso de los Estados Unidos no ha aplicado políticas claras y concisas para vigilar los servicios de inteligencia en los últimos años. Esto ha obedecido en gran parte a las trabas puestas por el sector privado, interesado en continuar siendo subcontratado por las agencias de inteligencia por ser un negocio que les representa enormes ganancias.

Es por ello que algunos analistas han sugerido que el primer paso debería ser que el Congreso destine presupuesto para el desarrollo de tecnología propia y capacitación de personal gubernamental para que las Agencias dejen de depender de las subcontrataciones. El gobierno norteamericano tiene la necesidad de reducir los gastos presupuestales de inteligencia por una parte y por otra establecer políticas más claras de vigilancia y supervisión, porque sería difícil esperar una rendición de cuentas de actividades que por definición son reservadas.

---

[181]Cita textual en ingles: "*the FISA Court, likewise, has found itself severely handicapped by the lack of information in its oversight efforts (…) the FISA Court is "forced to rely upon the accuracy of the information provided to the Court" and lacks the tools to independently verify how often the government's actions violate the court's rules".* Glenn Hastedt, *Evaluating Congressional Oversight of Intelligence*, [en línea], E-International Relations, 23 de agosto 2013, Dirección URL:http://www.e-ir.info/2013/08/23/evaluating-congressional-oversight-of-intelligence/, [Consultado el 24 de marzo de 2014].

Podría decirse que para que exista una verdadera supervisión de las actividades de inteligencia se necesita establecer claridad en las atribuciones del Ejecutivo y del Legislativo, así como en los mecanismos para establecer acuerdos entre los Comités de Inteligencia de ambas Cámaras. Establecer como requisito que los miembros de estos Comités cuenten con algún tipo de experiencia en el área de inteligencia, para que tengan una idea más clara de las acciones que deben realizar y establecer acciones conjuntas respecto a cuál debe ser la participación de las empresas subcontradas.

3.5 Subcontratación de empresas privadas en el manejo de información

El hecho de que se haya logrado filtrar información clasificada perteneciente al gobierno, también muestra que existen problemas en el funcionamiento de las agencias de inteligencia, los cuales se han complicado aún más con la subcontratación de empresas privadas para el manejo de la información.

Antes de los años noventa las agencias de inteligencia de los Estados Unidos principalmente la NSA contaba con sus propios técnicos en computación, criptógrafos, y analistas de información para manejar los sistemas de seguridad cibernética internos. Sin embargo, en los últimos 10 años el sector privado se ha convertido en el mayor distribuidor de herramientas y de personal para la Comunidad de Inteligencia. La CIA, la NSA y otras agencias reconocidas han recurrido a la subcontratación para el análisis de inteligencia y para realizar operaciones técnicas y de vigilancia[182].

El acelerado crecimiento de Internet y el desarrollo constante de la tecnología en los sistemas de telecomunicación dificultaron que las agencias de inteligencia se

---

[182] Cita textual en ingles: "*over the past ten years, the private sector has become a major supplier of tools and brainpower to the Intelligence Community. The CIA, the NSA, and others agencies once renowned for their analysis of intelligence and for their technical prowess in covert operations, electronic surveillance, and overhead reconnaissance have outsourced*" Tim Shorrock, Spies for Hire: The Secret World of Intelligence Outsourcing, o*p. cit*., p. 11.

mantuvieran a la vanguardia en los avances tecnológicos, lo que propició el buscar apoyo de las empresas privadas y de sus técnicos para realizar estas tareas[183].

Como ya mencionamos anteriormente la información clasificado a partir del 11 de septiembre de 2001 se resguardó en el programa SIPRENet. Sin embargo, la falta de capacitación del personal militar en este programa llevó a que civiles y contratistas externos tuvieran acceso a este sistema y a un gran número de información clasificada[184].

El incremento de la subcontratación privada obedeció a la experiencia con la que contaban empresas privadas como Oracle, AOL Time Warner, Hewlett-Packard y AT&T y a la calidad de sus técnicos. Adicionalmente, se sumaron a la vinculación sector público- privado, ofreciendo al gobierno de los Estados Unidos ayuda en la lucha contra el terrorismo, como una medida para construir nuevos sistemas de seguridad que mantuvieran protegido a los norteamericanos de cualquier ataque terrorista[185].

Entre 2002 y 2006 varias empresas privadas consiguieron nuevos contratos y se incrementó el número de empresas privadas dedicadas al manejo de información, pasando de 144 compañías en 2001 a 5,400 compañías en 2006. Algunas de las

---

[183] Cita textual en ingles: *"the Bush administration and Congress, determined to prevent further terrorist attacks, ordered a major increase in intelligence spending and organized to hire thousands of analysts and human intelligence specialists, (…) many of the people with the skills and security clearances to do that work were in the private sector. As a result, contracting grew by leaps and bounds as intelligence agencies rushed to fill the gap"* Tim Shorrock, *Spies for Hire: The Secret World of Intelligence Outsourcing*, Estados Unidos, Ed. Simon & Schuster, 2008, p. 35.

[184] Cita textual en ingles: *"Poor understanding of the system by many officials meant substantial quantities of material with no military connections also ended up on the system. Up to 3 million military and civilian employees, and external contractors, had access to some quantity of classified material through the network's"* Charlie Beckett; James Ball, *Wikileaks News in the Network Era*, Gran Bretaña, Ed. Polity Press, p.49.

[185]Cita textual en ingles: *"in the immediate aftermath of 9/11, a group of large technology companies, including Oracle, AOL Time Warner, Hewlett-Packard, and AT&T, approached the U.S. government to offer their assistance in the war against terror. The government has turned to technology providers to build new security systems".* Andrew Chadwich, *Internet Politics*, Estados Unidos, Ed. Oxford Press, 2006, p. 266.

principales compañías dedicadas a este rubro fueron Booz Allen Hamilton, *Science Applications International Corporation* (SAIC, siglas en ingles), BAE Systems y Lockheed Martin[186], quienes asistieron en la creación y vigilancia de programas de inteligencia más innovadores y seguros para garantizar el resguardo de la información gubernamental.

Sin embargo, la subcontratación de empresas privadas para el manejo de información secreta representa un peligro no sólo para el gobierno de los Estados Unidos, sino para los ciudadanos, ya que el hecho de que un gran número de personas tengan acceso a datos personales como lo plantea el Washington Post quien asegura que 856,000 funcionarios están autorizados para tener acceso a material clasificado[187], pone en peligro la privacidad de los ciudadanos. También abre la posibilidad de que estos datos puedan ser vendidos o utilizados con otros propósitos ya sea comerciales, políticos, electorales, etc., sin el consentimiento de los afectados.

Además esta subcontratación de empresas impide que sean supervisadas por el Congreso y no se tiene información sobre cómo están funcionando, qué actividades están realizando, así como de los presupuestos y gastos que tienen. Lo cual abre la posibilidad de que puedan realizar actividades más allá de las permitidas por la Constitución Norteamericana.

De acuerdo con el periódico Washington Post, de todo el personal con acceso a material clasificado, por lo menos un 31% son empleados privados, lo que significa que están jugando un papel fundamental dentro de la Comunidad de Inteligencia, sin ser esta su función. Se estima que de todo el personal con acceso a

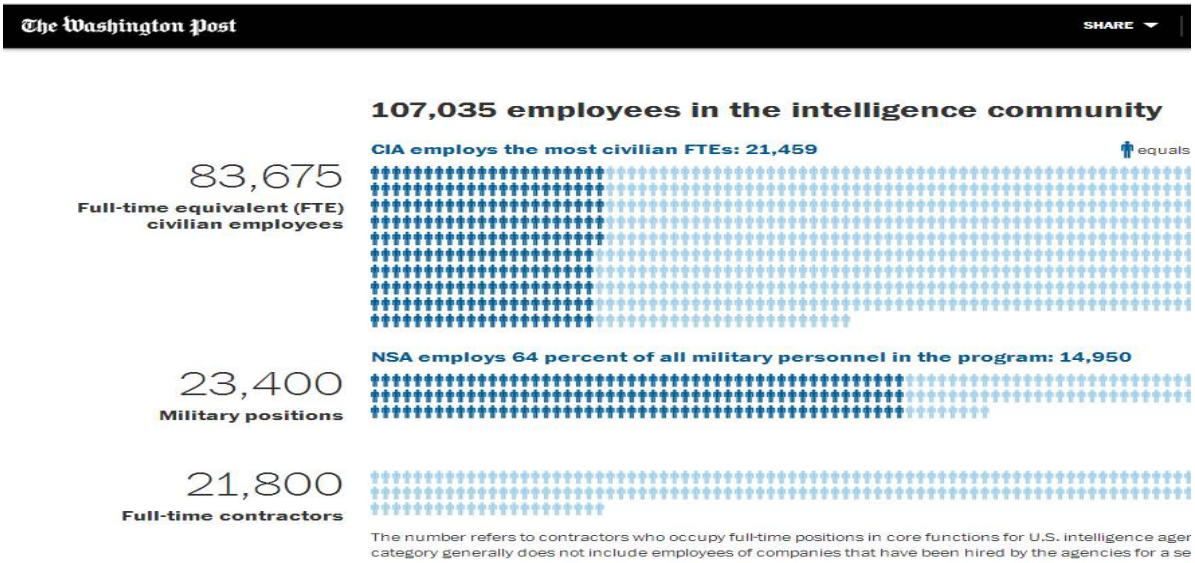
---

[186] Tim Shorrock, *Spies for Hire: The Secret World of Intelligence Outsourcing, op.cit*., p. 11.
[187] Cita textual en ingles: "*The Washington Post reported, that 856,000 officials had clearance for access to top-secret material".* Kinsman Jeremy, *Truth and consequence: The Wikileaks saga*, [en línea], Policy Options, Febrero 2011, Dirección URL:http://www.irpp.org/en/po/from-climate-change-to-clean-energy/truth-and-consequence-the-wikileaks-saga/, [Consultado el 25 de marzo de 2014].

información clasificada, 265,000 son contratistas privados[188]. Estos datos demuestran que un número importante de personas acceden a datos confidenciales y lo grave de esta situación es que no se está llevando un control del manejo que le están dando a esta información.

La Tabla 4 nos ejemplifica más claramente cómo en 2013 estaba funcionando la división de personal dentro de la comunidad de inteligencia de los Estados Unidos, donde del total de 107,035 empleados, 83,675 son civiles de tiempo completo, mientras que solamente 23,400 son militares, casi el mismo número que los empleados subcontratados quienes, son 21,800[189].

Tabla 5 Número de empleados de la Comunidad de Inteligencia



s/a, *The Black Budget*, [en línea], Estados Unidos, Washington Post, Dirección URL: http://www.washingtonpost.com/wp-srv/special/national/black-budget/, [Consultado el 19 de marzo de 2014].

---

[188] Cita textual en ingles: "*contractors are playing an ever more important role. The Post estimates that out of 854,000 people with top-secret clearance, 265,000 are contractors. There is no better example of the government's dependency on them than at the CIA".* Dana Priest; William M. Arkin, *National Security Inc.*, [en línea], Estados Unidos, Washington Post Investigation, Dirección URL:http://projects.washingtonpost.com/top-secret-america/articles/national-security-inc/, [Consultado el 18 de marzo de 2014].

[189] s/a, *The Black Budget*, [en línea], Estados Unidos, Washington Post, Dirección URL: http://www.washingtonpost.com/wp-srv/special/national/black-budget/, [Consultado el 19 de marzo de 2014].

Igualmente, esta subcontratación de empresas está generado otros problemas. Las empresas privadas están pagando mayores sueldos a sus trabajadores y ello ha ocasionado que el gobierno cuente con un personal de inteligencia con menos experiencia, ya que los más capacitados han optado por el sector privado[190], debido a que reciben mejores salarios y trabajan menos tiempo.

El tema es controvertido y ha llevado a especular sobre cuáles son las razones por las cuales se continúa incrementando la subcontratación privada. Una de las posturas plantea que tomando en cuenta las ganancias económicas que están recibiendo las empresas privadas, algunos miembros de la misma comunidad de inteligencia gubernamental se han convertido en colaboradores y accionistas de estas compañías subcontratadas y por lo tanto promueven su injerencia. Ejemplo de ello es el actual Jefe de Inteligencia Nacional de los Estados Unidos, James Clapper, quien es también ejecutivo de la empresa Booz Allen. Mientras que su antecesor en el puesto Mike McConnell es actualmente vicepresidente de Booz Allen. De igual forma el actual director de la CIA, James Woolsey es también vicepresidente de esta compañía[191]. Estos datos evidencian que existe una estrecha relación entre el sector privado y el sector público en esta materia, lo que pone a discusión si las agencias están velando por los intereses del gobierno norteamericano (seguridad) o por sus intereses personales (ganancias económicas).

---

[190]Cita textual en ingles: "*the government has been left with the youngest intelligence staffs ever while more experienced employees move into the prívate sector."* Dana Priest; William M. Arkin, *National Security Inc*., *op. cit*. p. 2.

[191]Cita textual en ingles: *"the current head of U.S national intelligence (DNI), James Clapper, is a former Booz Allen executive, while the man he took over from as DNI, Mike McConnell, is the current vice-chairman of the firm. Former CIA director James Woolsey was also a vice president of the company"* Aubrey Bloomfield, *Booz Allen Hamilton : 70 % of the U.S. Intelligence Budget Goes to Private Contractors*, [en línea], PolicyMic, Dirección URL:http://www.policymic.com/articles/48845/booz-allen-hamilton-70-of-the-u-s-intelligence-budget-goes-to-private-contractors, [Consultado el 19 de marzo de 2014].

En un principio cuando se comenzó a incrementar la contratación de empresas privadas se pensaba que esto significaría mayores ventajas y menores costos para el gobierno federal y ello aceleró una mayor subcontratación en materia de inteligencia. Sin embargo, a mediano plazo observamos que un alto porcentaje del presupuesto de inteligencia quedó en manos de empresas privadas[192]. Incluso, el Senado de los Estados Unidos ha destacado que esta subcontratación resulta más cara que tener empleados de tiempo completo[193].

Es por ello que durante la administración de Barack Obama se han realizado esfuerzos para disminuir la subcontratación de empresas privadas en materia de inteligencia[194]. Sin embargo, *a* pesar de tales los esfuerzos el número de empresas contratadas y de personal subcontratado aún es muy alto y sigue generando altos costos en el presupuesto de las agencias de inteligencia.

Finalmente, la subcontratación genera una larga cadena de personal que tiene acceso a información clasificada, lo cual complica el monitoreo y seguridad de toda esa información[195] lo que lleva a que sea más fácil una filtración, ya que no

---

[192]Cita textual en ingles:*"government contractors [are] doing what are essentially governmental jobs, (…) Seventy percent of America's intelligence budget now flows to private contractors".* Tim Shorrock, Put the Spies back under one roof, o*p.cit.,* Dirección URL:http://www.nytimes.com/2013/06/18/opinion/put-the-spies-back-under-one-roof.html?ref=centralintelligenceagency, [Consultado el 26 de marzo de 2014].

[193]Cita textual en ingles:*"the spy community had bolstered its work forces by 20% since the September 11 attacks, (…) While companies and agencies typically outsource functions to save money, the Senate intelligence committee found that contractors are more expensive than full-time government employees".* Spencer Ackerman, *Snowden leak shines light on US intelligence agencies' use of contractors*, [en línea], The Guardian, 10 de junio 2013, Dirección URL:http://www.theguardian.com/world/2013/jun/10/edward-snowden-booz-allen-hamilton-contractors, [Consultado el 25 de marzo de 2014].

[194]Cita textual en ingles: "*the idea that contractors cost less has been repudiated, and the administration has made some progress toward its goal of reducing the number of hired hands by 7 percent over two years"* Dana Priest; William M. Arkin, *op.cit.,* p.1, Dirección URL:http://projects.washingtonpost.com/top-secret-america/articles/national-security-inc/, [Consultado el 25 de marzo de 2014].

[195]Cita textual en ingles: "*as more individuals handle more secrets in more places around the world, it naturally becomes harder to keep track of them."* Massimo Calabresi, *Wikileaks'War on Secrecy: Truth' consequences*, [en línea], Estados Unidos, TIME Magazine, 2 de diciembre 2010, Dirección URL: http://content.time.com/time/magazine/article/0,9171,2034488,00.html, [Consultado el 30 de marzo de 2014].

se puede tener total certeza de que el personal de las empresas contratadas estén siguiendo los estándares de confidencialidad y seguridad que deben mantener las agencias de inteligencias. El problemas se hace mas complejo porque estas empresas privadas no tienen ninguna obligación de rendir cuentas ante ninguna instancia gubernamental sobre su desempeño, actividades e ingresos, lo cual genera más posibilidad de realizar acciones ilegales en materia de inteligencia o de uso inadecuado de la información.

En conclusión podemos decir que la filtración de los cables diplomáticos por parte de Wikileaks generó cuestionamientos internos dentro del gobierno de los Estados Unidos al evidenciar que existen algunos problemas dentro de estas políticas de seguridad cibernética. El Congreso no está llevando una estricta supervisión de las actividades emprendidas por las agencias de inteligencia, las cuales han recurrido desde hace varios años a la subcontratación de empresas privadas para realizar actividades de responsabilidad federal. Además de demostrar que se está gastando una gran parte del presupuesto federal a las actividades de inteligencia.

Capítulo 4 El caso de Wikileaks y las consecuencias externas de los *Cablegates*

El objetivo de este capítulo es destacar que a pesar de que en la opinión pública la filtración de los cables de Wikileaks tuvieron relevancia, al reactivar la discusión sobre si las actividades de espionaje emprendidas por las agencias de inteligencia son una violación a los derechos humanos vs la seguridad nacional, las revelaciones no tuvieron un impacto directo a nivel diplomático.

Para comenzar con este capítulo se hará un breve recuento de lo implicó Wikileaks y las dificultades para utilizar la información de los cables diplomáticos.

En primer lugar debemos destacar que la revelación de la información confidencial por parte de Wikileaks a través de una página de Internet fue un aspecto novedoso por su alcance, ya que cualquier ciudadano puede consultar directamente los documentos de forma instantánea. Sin embargo, debemos precisar que su popularidad no se debió a esta particularidad, sino a que esta organización recurrió a algunos de los principales periódicos del mundo para darle mayor difusión en el ámbito internacional y darle más trascendencia a esta información, al depurarla y seleccionarla, lo cual contribuyó a ampliar su impacto, demostrando de esta manera que aún las asociaciones independientes e Internet necesitan la ayuda de los medios de comunicación de cierto prestigio, para darle mayor difusión a la información.

> *"La asociación con estos diarios permitió a Wikileaks maximizar la difusión de la megafiltración a niveles que no hubieran tenido lugar sin la transferencia de prestigio editorial, oficio periodístico y credibilidad en la comunidad (…) Así, pues en lugar de reemplazo tecnológico, fue la colaboración entre el uso de Internet, como sinónimo de la velocidad y de manejo de gigantescos volúmenes de datos, y los viejos*

medios, con sus potencias editoras y sus rutinas secuenciales, lo que se conjugó como estrategia de alto impacto [...]"[196].

Este hecho mostró que la información en el ciberespacio requiere una guía, particularmente cuando es voluminosa, y se tienen diversos niveles de información tanto personal; de situaciones de corrupción, violaciones a derechos humanos; seguridad nacional; intereses económicos, etc., de diferentes países y de diferentes épocas.

Adicionalmente "[...] los cables diplomáticos hacen referencia "pasado y presente, aludiendo a hecho de la historia reciente que, en muchos casos, repercuten en la actualidad; amenaza con socavar los cimientos de algunas viejas certezas del oficio periodístico [...]"[197], demostrando que la filtración de información clasificada puede traer como consecuencia la reactivación de viejas discusiones, sobre temas sensibles de la agenda internacional pero también en torno a la trasparencia y difusión de datos confidenciales.

Por otra parte, es preciso hacer mención de las dificultades que se presentan al revisar los documentos dentro del portal de Internet, al momento de tener su primer acercamiento a los cables de Wikileaks. En primer lugar, por el volumen de información y la variedad de las temáticas que se abordan a lo largo de aproximadamente trece años, que hace más complicado el manejo y análisis de los cables. Ya que si bien es cierto el portal de Internet donde se encuentra almacenada toda la información[198] brinda la posibilidad de filtrar la información ya

---

[196] Prólogo de Martín Becerra en Santiago O'Donnell, ArgenLeaks, Buenos Aires, Ed. Ramdom House Mondadori, S.A., [en línea], 2011, Dirección URL: http://books.google.com.mx/books?id=fA3c1tEgaF4C&printsec=frontcover&dq=wikileaks&hl=es&sa=X&ei=BYbyU5iNKcPR8AGO5oHgCg&ved=0CEQQ6AEwBQ#v=onepage&q=wikileaks&f=false, [Consultado el 18 de agosto 2014].

[197] Prólogo de Martín Becerra en Santiago O'Donnell, ArgenLeaks, *op.cit.*

[198]Véase Cablegate's cables: Full-text search everything, Dirección URL: https://cablegatesearch.wikileaks.org/search.php#c1, [Consultada el 9 de mayo 2014].

sea por fecha, por país de origen, por clasificación de confidencialidad, esto no es suficiente para hacer una verdadera depuración de información.

En segundo lugar el manejo de estos documentos se dificulta porque los cables están descontextualizados, así que al momento de leerlos por primera vez si no se tiene de antemano un conocimiento de la situación del país y de sus principales gobernantes, no se entiende a qué tema o a qué persona están haciendo referencia e incluso esto puede llevar a interpretaciones erróneas.

La publicación masiva de documentos de secretos militares y diplomáticos no convierte a Wikileaks en un medio periodístico, ya que ello hubiera requerido de realizar una reflexión y contextualización de la información que conecte los documentos con las realidades locales.

También debemos tener en cuenta que se desconoce el uso que el gobierno norteamericano le dio a la información, ya que estamos hablando de una base de datos que no nos brinda información sobre las estrategias políticas de las autoridades, ni sobre las peticiones que los diplomáticos respondieron, Incluso, no hay pruebas claras de que la información es fidedigna, porque aparece sin fuentes, por lo tanto su nivel de veracidad se puede poner en duda. Sin embargo, el hecho de que las autoridades hayan evadido responder cuestionamientos sobre la autenticidad de la información, ha operado como reafirmador de que es certera, aunque en realidad no existe prueba de ello.

Es por estas razones que para analizar la información se establecerá una clasificación basada en el tipo de documentos que fueron expuestos por Wikileaks para hacer más sencillo el manejo de la información, la cual se enumera a continuación: 1) documentos en lo que se exponen la situación de corrupción por parte de las autoridades de los distintos niveles, violación a derechos humanos e impunidad, 2) cables que hablen sobre la opinión personal de los diplomáticos sobre sus homólogos o de presidentes de otros países, 3) información relacionada

con intereses económicos de Estados Unidos en el exterior en distintas materias, 4) documentos relacionados con cuestiones de seguridad nacional.

4.1 Trascendencia de Wikileaks y las críticas a los diplomáticos

La revelación de estos cables fue relevante, porque demostró que el gobierno de los Estados Unidos mantenía una política de espionaje y recolección de información en todo el mundo, no sólo de las posturas ideológicas y políticas, sino también de las personales. También confirmó que aún hoy en día las actividades de inteligencia son prioritarias para el gobierno de los Estados Unidos.

Asimismo estas políticas de espionaje generaron cuestionamientos al evidenciar que no se están respetando los Tratados Internacionales en materia de información reservada y confidencial. El problema de la vigilancia electrónica es que por un lado, pone a discusión el espionaje y por el otro el límite entre lo privado y lo público, porque no permite ejercer cierto control sobre lo que queremos que el mundo sepa de nosotros[199].

Es decir, que el problema no es solamente mantener resguardada información bajo el principio de la preponderancia de la seguridad nacional, sino que se pone a discusión el hecho de que las agencias de inteligencia tengan acceso a información reservada, la cual al ser difundida viola la privacidad de las personas y de los funcionarios públicos, al hacer uso de sus datos personales, ideología y actividades.

El caso de Wikileaks también generó dificultades dentro del marco de las negociaciones internacionales, particularmente porque al darse a conocer esta información los actores involucrados disponen de mayor información que también

---

[199]Cita textual en ingles: *"the problem with ubiquitous electronic surveillance is not that we have a simple dislike of being watched; it is that the distinction between private and pubic expression allows us to exert some control over how we would like the world to see us."* Andrew Chadwich*, Internet Politics*, Estados Unidos, Ed. Oxford Press, 2006, p. 263.

podrán utilizar para presionar al gobierno norteamericano tanto en el terreno económico como en el político. Debido a que "[…] recabar esta información posibilitaba el chantaje o presionar a las personas a la que el estado espiaba"[200]. Ahora también los países cuentan con indicadores más claros de la relevancia geopolítica que las diversas zonas del mundo tienen para el Estado norteamericano, lo cual se convierte en información estratégica.

Este hecho fue reconocido por la propia Secretaria de Estado, Hillary Clinton, quien afirmó que la filtración de Wikileaks significó un importante golpe contra los esfuerzos de Estados Unidos para trabajar con otros países en el afán de solucionar problemas comunes y por tales razones esto significaba un golpe para la comunidad internacional. Ya que estas revelaciones fueron no solo un ataque a la política exterior estadounidense, sino contra las alianzas, convenciones y negociaciones internacionales que salvaguardan la seguridad global y mantiene la estabilidad mundial[201]. Es decir, desde la perspectiva del gobierno norteamericano esta información no solamente afectó la seguridad nacional, sino también las relaciones económicas, políticas y diplomáticas de su país con otras naciones.

En apariencia se podría hablar de que Wikileaks tuvo gran trascendencia porque abrió a nivel internacional la discusión sobre la aplicación del principio de máxima transparencia (contra la cultura del secreto). También abrió la discusión sobre el delito de difundir información reservada del Estado sin la previa autorización del mismo y la falta de sanciones hacia un Estado que obtiene información por la vía del espionaje. Estas discusiones parecen un callejón sin salida porque en el fondo refleja dos posiciones políticas encontradas, la de los que no tienen poder y la de los que lo ejercen.

---

[200] Ana María Salazar, o*p.cit*, Pp. 170-171.
[201] Cita textual en ingles: *"This disclosure is not just an attack on America's foreign policy; it is an attack on the international community, the alliances and partnerships, the conventions and negotiations that safeguard global security and advance economic prosperity"*. CNN Wire Staff, *Clinton condemns leak as 'attack on international community'*, [en línea], CNN U.S., 30 de noviembre 2010, Dirección URL: http://www.cnn.com/2010/US/11/29/wikileaks/, [Consultado el 20 de abril 2014].

Los que han apoyado este primer argumento han sido en su mayoría periodistas, académicos y Organizaciones No Gubernamentales. Ellos plantean que Wikileaks permite conocer abusos y corrupción presentes en los gobiernos de varios países, que es un derecho de los ciudadanos saber lo que su gobierno hace y sus prioridades, ya que la transparencia en un principio rector del estado democrático. Algunos actores como Amnistía Internacional se pronunciaron en favor de publicar la información en contra de la violación de los derechos humanos

> *"[…] acoge con satisfacción los esfuerzos por hacer de dominio público la información sobre abusos contra los derechos humanos (…) nos gustaría poner de relieve que la libertad de expresión incluye el derecho a recibir y difundir toda clase de información, con excepciones estrechamente definidas"*[202].

Al reconocer que Wikileaks puede servir como mecanismo de presión para evitar la reiteración de violaciones, se busca desmontar las supuestas conspiraciones del poder y/o democratizar al Estado, así como lograr un empoderamiento y encontrar nuevos espacios para otros sectores no pertenecientes al gobierno, "(…) los gobiernos nacionales deben adoptar medidas activas a fin de asegurar el principio de máxima transparencia, derrotar la cultura del secreto que todavía prevalece en muchos países y aumentar el flujo de información sujeta a divulgación"[203], al considerar que esta es la única manera para lograr una verdadera democracia.

La opinión pública argumentó en rechazo al bloqueo y censura del portal de internet de Wikileaks porque

---

[202]Amnistía Internacional España, *Wikileaks y la libertad de expresión. Preguntas y respuestas,* [en línea], Amnistía Internacional, 9 de diciembre de 2010, Dirección URL:https://www.es.amnesty.org/noticias/noticias/articulo/wikileaks-y-la-libertad-de-expresion-preguntas-y-respuestas/, [Consultado el 30 de abril de 2014].

[203] Relatores especiales de la OEA y ONU, *Declaración Conjunta sobre Wikileaks*, [en línea], OEA, 21 de diciembre 2010, Dirección URL:http://www.oas.org/es/cidh/expresion/showarticle.asp?artID=829&IID=2, [Consultado el 31 de abril de 2014].

"[…] los bloqueos o sistemas de filtración de Internet no controlados por usuarios finales, impuestos por un proveedor gubernamental o comercial del servicio son una forma de censura previa y no pueden ser justificados. Las empresas que proveen servicios de Internet deben esforzarse para asegurar que se respeten los derechos de sus clientes de usar Internet sin interferencias arbitrarias"[204].

Es decir, que la decisión de intervención en Internet fue vista como un atentado contra la libertad de prensa y expresión por parte del gobierno norteamericano. Otros argumentaron que "la red es la herramienta más poderosa para que los ciudadanos en las sociedades democráticas pongan en práctica una supervisión completa sobre las actividades de sus teóricos, representantes, los políticos"[205].

En contraste, el gobierno de los Estados Unidos bajo el principio de que la filtración de información es un delito que atenta contra la seguridad nacional y el principio de secreto de Estado[206], consideran que Wikileaks es una amenaza peligrosa para la seguridad del Estado y se debía evitar su difusión[207]. Debido a que "existe información que es demasiado delicada para poder revelarla, pues se puede convertir en la mejor arma para que una potencia hostil realice un ataque efectivo"[208]. Se argumenta que las personas que realizan estas filtraciones bajo la

---

[204]Relatores especiales de la OEA y ONU, *Declaración Conjunta sobre Wikileaks,* OEA, 21 de diciembre 2010, Dirección URL:http://www.oas.org/es/cidh/expresion/showarticle.asp?artID=829&lID=2, [Consultado el 2 de mayo 2014].

[205] Assange Julian, *Cypherpunks: La libertad y el futuro de internet, España*, Ed. Deusto, 2012, p. 10.

[206]Cita textual en ingles: *"constitutes a dangerous, illegal disruption to state security and operations that must be stopped by any means possible."* Yochai Benkler, A Free Irresponsible Press: Wikileaks and the Battle over the Soul of the Networked Fourth Estate en Fenster Mark,Disclosure's, *Effects: WikiLeaks and Transparency*, Revista Iowa Law Review, Universidad de Iowa, Vol. 97:753, 2012, p. 759, Dirección URL:http://www.uiowa.edu/~ilr/issues/ILR_97-3_Fenster.pdf, [Consultado el 1 de mayo de 2014].

[207]Cita textual en ingles: *"constitutes a dangerous, illegal disruption to state security and operations that must be stopped by any means possible."* Yochai Benkler, A Free Irresponsible Press: Wikileaks and the Battle over the Soul of the Networked Fourth Estate en Fenster Mark,Disclosure's, *Effects: WikiLeaks and Transparency*, Revista Iowa Law Review, Universidad de Iowa, Vol. 97:753, 2012, p. 759, Dirección URL:http://www.uiowa.edu/~ilr/issues/ILR_97-3_Fenster.pdf, [Consultado el 29 de abril 2014].

[208] Ana María Salazar, o*p.cit,* Pp. 121-122.

premisa de colaborar con la trasparencia de las actividades gubernamentales, generalmente no analizan las implicaciones que tienen las filtraciones para las personas involucradas en materia de política exterior, porque tanto los enemigos como los aliados pueden utilizar esta información en contra del gobierno norteamericano. Y como lo vimos en capítulos anteriores la resultante consiste en desarrollar nuevos métodos para garantizar el secreto de las comunicaciones y nuevas prácticas para la gestión de la información militar, diplomática y corporativa, tratando de evitar las fugas.

Esto también ha ido acompañado de la difusión de argumentos en favor del espionaje, como se evidencia en un artículo del *Center for Strategic & International Studies,* donde se plantea que estas actividades de espionaje no son una violación, ya que consideran que la intimidad no es absoluta, y que la interferencia es admisible si no se hace de manera arbitraria, es decir si se hace bajo supervisión y de manera legal[209]. Este centro de estudios argumenta que los trabajos realizados por las Agencias de Inteligencia no violan este derecho a la privacidad, ya que han sido diseñados para investigar a las posibles amenazas hacia los Estados, pero sin violar los estándares de privacidad.

Es por ello que el gobierno de los Estados Unidos adoptó la posición de desprestigiar no solamente a Wikileaks como organización sino a su creador Julian Assange por difundir esta información. El gobierno emitió una orden judicial para bloquear todas las señales de emisión de esta organización dentro de Internet, para que no se pudiera tener acceso a la información. Sin embargo, la decisión fue blanco de críticas por parte de distintos sectores, por lo que la decisión al final fue revertida, al crearse páginas espejo donde se encontraba la misma información pero con otra dirección electrónica.

---

[209]Cita textual en ingles: "*privacy is not absolute, interference is permissible if it is not arbitrary, the antonyms of arbitrary include oversight and constitutional*". James Andrew Lewis, *Simple Tests for Surveillance*, [en línea], Center for Strategic & International Studies (CSIS), 12 de Junio 2013, Dirección URL: https://csis.org/publication/simple-tests-surveillance, [Consultado el 7 de octubre de 2013].

La filtración de estos cables diplomáticos también generó cuestionamientos sobre el papel que desempeñan los diplomáticos norteamericanos en el exterior. Al demostrar las contradicciones del gobierno de los Estados Unidos sobre lo que dice de manera pública y lo que dice a puertas cerradas[210]. Además significó el reconocimiento de que una de las funciones de los diplomáticos es espiar a sus contrapartes y ello ha generado fuertes reacciones por parte de los jefes de estado de otros países.

Es preciso también mencionar que el caso de Wikileaks manifestó que bajo el principio de protección de la seguridad nacional y lucha contra el terrorismo, el gobierno de los Estados Unidos ha cometido actos ilegales de manera abierta y cotidiana, al espiar conversaciones privadas. Si bien es cierto que las actividades de espionaje no son una actividad nueva para los norteamericanos, se vuelve trascendental que se sigan realizando, particularmente porque la realidad internacional actual ya no es la de Guerra Fría, donde se utilizaban políticas de espionaje contra los opositores, bajo el argumento de protección contra el enemigo en esta lucha ideológica-política. En la actualidad ya no existen estos conflictos ideológicos y existe una supuesta estabilidad internacional, lo cual genera cuestionamientos sobre la manera en la que el gobierno de los Estados Unidos continúa utilizando estas políticas de espionaje para conseguir ventajas comparativas, al momento de negociar y establecer pactos o alianzas con otros gobiernos.

Además el fenómeno de Wikileaks puso en evidencia que el gobierno norteamericano tiene un discurso público y uno oculto. Este último basado en el principio de asegurar la hegemonía norteamericana dentro de la sociedad

[210]Cita textual en ingles: "*This documents release reveals the contradiction between the US's public persona and what it says behind closed doors- and shows that if citizens in a democracy want their government to reflect their wishes, they should ask to see what's going on behind the scenes."* Charlie Beckett; James Ball, o*p. cit*,, p.49.

internacional[211]. Al mismo tiempo la filtración de estos cables mostró la realidad de las discusiones internacionales. En la opinión pública se realizan valoraciones superficiales sobre las autoridades estatales sin tomar en cuenta los protocolos, lo cual en algunas ocasiones puede generar roces y fricciones entre los Estados.

Finalmente, estos cables rompieron con uno de los mitos de la política exterior estadounidense de integridad y trasparencia de los diplomáticos. También se mostró que el gobierno de los Estados Unidos está informado sobre los problemas de corrupción y los graves problemas internacionales y sin embargo, continúa manteniendo esta información en secreto para su uso estratégico.

4.2 Consecuencias Externas de los *Cablegates*

En el caso de los *Cablegates* de Wikileaks existen diferentes opiniones sobre las consecuencias externas que trajo consigo la filtración de cables diplomáticos, algunos consideran que los cables no revelan nada novedoso que solo ratifican información previamente conocida, al no demostrar importantes negociaciones detrás de escena y consideran que la filtración de los *Cablegates* solo constituye un chisme, porque no se puede confirmar a través de pruebas concretas su validez.

Lo que si podemos comprobar es que la filtración de los *Cablegates* por parte de Wikileaks generó un deterioro de la imagen de los diplomáticos ante la opinión pública, que quedaron evidenciados como los principales espías en el extranjero. Ante lo cual este sector argumentó en su favor que estaban dedicándose a encontrar terrenos comunes con los gobiernos extranjeros para resolver lo que

[211] Salvador Martí, Wikileaks y América Latina: el discurso oculto de los poderosos, Nueva Sociedad, Buenos Aires, Febrero 2011, p.4.

ellos consideran sus retos compartidos[212] y que su propósito era preservar los intereses de los Estados Unidos y proteger su seguridad nacional.

Argumentaron que filtrar información clasificada no contribuye al progreso de los intereses de los Estados Unidos[213], porque el tratamiento de información clasificada por personas ajenas a esta tarea puede prestarse a malas interpretaciones, al no conocer cuáles son los propósitos y la razón por la cual se enviaron estos cables.

El fondo de la discusión es si puede haber diplomacia efectiva sin confidencialidad, ya que el proceso histórico de la diplomacia nos ha mostrado la presencia de esta dinámica secreta en diversas ocasiones, como un medio para lograr negociaciones internacionales exitosas que de haberse hecho públicas es difícil asegurar que se hubieran consumado. Adicionalmente, Wikileaks generó controversia porque rompió con la separación entre diplomacia, periodismo y otras formas de comunicación[214], al integrar la información en un solo sitio sin un análisis ni contextualización previa.

---

[212]Cita textual en ingles: "*rather than pulling strings behind the scene, American diplomats struggle to find commond ground with foreign governments to solve shared challenges. That presumably is what a leading global power should be doing.*" Lindsay James M., *Anglo-U.S. Relations can overcome Wikileaks fallout*, [en línea], Council on Foreign Relations, 2 de diciembre 2010, Dirección URL:http://blogs.cfr.org/lindsay/2010/12/03/anglo-u-s-relations-can-overcome-wikileaks-fallout/, [Consultado el 17 de mayo 2014].

[213]Cita textual en ingles: "*Our diplomacy's ultimate purpose is to advance the interests of the United States and preserve our national security, as defined by a freely elected government. Those who leak classified documents are asserting that they know better what is in the United States collective interest than the government."* Markey Daniel S., *Will Wikileaks hobble U.S. Diplomacy?,* [en línea], Council on Foreing Relations, 1 de diciembre 2010, Dirección URL:http://www.cfr.org/diplomacy-and-statecraft/wikileaks-hobble-us-diplomacy/p23526, [Consultado el 20 de mayo 2014].

[214] Cita textual en ingles: "*The line between diplomacy, journalism, and other forms of international communication become especially indistinct with the publication, of (…) classified diplomatic cables by the WikiLeaks web site*". Andrew F. Cooper; Jorge Ieine; Ramesh Thakur, *The Oxford Handbook of Modern Diplomacy*, Reino Unido, Ed. Oxford University Press, 2013, p. 455

La filtración de los cables no sorprendió a los expertos en el tema, sino que más bien lo que ha llamado la atención es que se deje huellas por escrito a través de cables de las comunicaciones entre embajadas y el gobierno federal. Sin embargo esto se explica, porque en las últimas dos décadas la diplomacia moderna de los Estados Unidos adoptó los sistemas digitales como el medio para establecer comunicaciones para la trasmisión, recepción y aseguramiento de información, al considerar que era un medio confiable y más rápido para comunicarse con otras partes del mundo, lo cual has sido puesto a discusión tras lo ocurrido.

El caso Wikileaks mostró que aun teniendo las mejores tecnologías las comunicaciones dentro de la red no estarán nunca completamente aseguradas, ya que existen riesgos evidentes. Esto fue afirmado en los siguientes términos: "A pesar de la utilización de las más modernas tecnologías al alcance del ser humano, como los ordenadores más potentes, los teléfonos vía satélite, terminan, tal como demuestran los cables diplomáticos filtrados a la prensa, quedando en manos del elemento más importante e imprescindible: el factor humano"[215].

Sin embargo, más allá de las tensiones diplomáticas, los enojos y susceptibilidades que estos cables generaron, el verdadero daño que trajo como consecuencia Wikileaks será que los informes diplomáticos van a ser menos sinceros, ya que los diplomáticos de otros países cuidarán más la información y los comentario que brinden a sus homólogos estadounidenses. Esto podría significar la perdida de información certera por parte de los diplomáticos estadounidenses[216]. Es decir, que ahora será mucho más complicado para los diplomáticos conseguir información sobre la situación que prevalece en el país en

---

[215] Juan Carlos Herrera Hermosilla, *Breve Historia del Espionaje*, España, Ediciones Nowtilus, 2012, p. 279.

[216]Cita textual en ingles: "*a less candid when talking with their American counterparts. US officials will resort to more euphemisms when they report back home. Washington will further restrict who gets what information*" James M. Lindsay, *Anglo-U.S. Relations can overcome Wikileaks fallout*, [en línea], Council on Foreign Relations, 2 de diciembre 2010, Dirección URL:http://blogs.cfr.org/lindsay/2010/12/03/anglo-u-s-relations-can-overcome-wikileaks-fallout/ , [Consultado el 29 de abril de 2014].

el que se encuentran, porque los dirigentes y el personal se volverán más herméticos sobre la información que les den a conocer, lo que podría dificultar el establecimiento de acuerdos entre las partes en materia diplomática. Esto podría convertirse en un grave problema para la política exterior norteamericana, ya que podría disminuir el suministro de información que es una base fundamental para las negociaciones y alianzas que emprende el gobierno norteamericano con el resto del mundo.

También podemos observar que a pesar de que muchos de los cables daban información delicada sobre algunos mandatarios, las consecuencias por estas filtraciones fueron menores y en la mayoría de los casos no generaron graves tensiones diplomáticas. Los mandatarios involucrados se mantuvieron serenos y aceptaron las explicaciones y disculpas dadas por el gobierno de los Estados Unidos sin generar mayores cuestionamientos sobre el tema.

En algunos casos la opinión pública manifestó su indignación y solicitó explicaciones a sus gobiernos por sus acciones, evasiones, corrupciones y malas prácticas. Es decir, las filtraciones de información más que debilitar al gobierno norteamericano afectó a algunos gobiernos nacionales, particularmente aquellos en los que la información dada a conocer operó como elemento de prueba de las irregularidades prevalecientes dentro del gobierno.

En los 250,000 cables dados a conocer por Wikileaks se aborda información sobre casi todos los países con los que Estados Unidos mantiene relaciones diplomáticas, lo cual muestra los excesos a los que han llegado las políticas de espionaje. Por cuestiones de metodología para esta investigación solamente analizaremos la información de algunos países de cada región, los cuales ejemplifican más claramente las tensiones diplomáticas que se generaron tomando en consideración la información que revelaron.

Para demostrar la hipótesis de que no en todos los países hubo un efecto diplomático se analizarán los casos de Egipto, Iraq y Afganistán (War Logs),

China, Corea del Norte, Alemania, Italia y Argentina, donde la filtración no generó consecuencia diplomática, se recurrirá a información secundaria, es decir proveniente de los medios de comunicación. Sin embargo, en los casos de México y Ecuador en donde se destituyó a los diplomáticos de ese momento nos remitiremos a la fuente original, para de esta manera comprender mejor el tipo de información señalada y el contexto de estos informes.

En primer lugar se presentará un cuadro comparativo que demuestra cuales fueron las principales consecuencias tanto internas como diplomáticas tras la filtración de estos cables, para probar que fueron mayores las consecuencias internas que las diplomáticas.

4.2.1 Egipto

En el caso de Egipto los cables demuestran que Washington se mostraba preocupado por la falta preparación sobre la sucesión de Mubarak, que seguía una postura muy dura. “Los cables también muestran que Washington considera a Egipto como un importante (…) aliado estable en diversas cuestiones, que incluyen el programa nuclear de Irán, la promoción de las negociaciones entre Israel y la Autoridad Palestina, y en la tarea de hacer una vida difícil a Hamas en Gaza”[217]. La posición de Mubarak en contra de las armas nucleares de Irán y su influencia sobre Hamas en Gaza y Hezbollah en Líbano parecen ser aspectos por los cuales el gobierno norteamericano lo considera un socio útil en Medio Oriente.

Y a pesar de ello, demuestra que “EU muestra frustración con la negativa de Mubarak de abordar los temas de derechos humanos. En 2008 habría dicho: “Mientras Egipto ha hecho mejoras limitadas en los últimos años, como la libertad

[217] Tim Lister, *El presidente de Egipto sigue siendo un aliado vital de EU, dice WikiLeaks*, [en línea], CNN México, 28 de enero de 2011, Dirección URL: http://mexico.cnn.com/mundo/2011/01/28/el-presidente-de-egipto-sigue-siendo-un-aliado-vital-de-eu-dice-wikileaks, [Consultado el 27 de marzo de 2014].

de prensa**,** el progreso en general ha sido lento"[218], además de evidenciar graves problemas internos dentro del gobierno de Mubarak, ya que el ejército está muy dividido[219], y existe "brutalidad policial en Egipto contra criminales comunes es rutinaria y lo impregna todo. Contactos describen el uso de la fuerza por parte de la policía para conseguir confesiones de criminales como algo diario, resultado de una formación pobre y de la falta de personal"[220]. Es decir, la falta de respeto a los derechos humanos es una problemática fundamental de este aliado.

Los *Cablegates* señalaron que a pesar de que han pasado ya más de diez años después de los ataques terroristas del 11 de septiembre en Estados Unidos, aún prevalecen sombras dentro de las relaciones entre los Estados Unidos y el Medio Oriente. Y es por esta razón que el gobierno de estadounidense se encuentra muy interesado en conocer la situación de esta región.

No se generaron importantes tensiones diplomáticas, pero las filtraciones si contribuyeron a incrementar el malestar de la población contra el gobierno interno por las irregularidades cometidas por sus autoridades. Es decir, en el caso de Egipto los efectos no fueron externos sino internos, al evidenciar los abusos de poder de los dirigentes que se enriquecían, mientras la población vivía en situaciones precarias.

4.2.2 War Logs

Si bien es cierto que los cables sobre información de Iraq y Afganistán conocidos como *War Logs* donde se registraban más de 92,000 acciones militares por parte

---

[218] Ibidem. Dirección URL: http://mexico.cnn.com/mundo/2011/01/28/el-presidente-de-egipto-sigue-siendo-un-aliado-vital-de-eu-dice-wikileaks,

[219] EFE, *Unos cables de WikiLeaks describen un Ejército egipcio dividido en fracciones,* [en línea], 20 minutos, es, 5 de febrero 2011, Dirección URL:http://www.20minutos.es/noticia/950658/0/wikileaks/ejercito/egipto/, [Consultado el 28 de marzo de 2014].

[220] Cable 09CAIRO79, Embajada estadounidense en El Cairo, 15 de enero de 2009, Confidencial, Dirección URL:http://www.tercerainformacion.es/spip.php?article21992, [Consultado el 27 de marzo de 2014].

de Estados Unidos en Afganistán realizadas entre enero de 2004 y diciembre de 2009, no pertenecen a las revelaciones proporcionadas por los *Cablegates,* esta información permite tener evidencia de las actividades del gobierno de los Estados Unidos durante las intervenciones militares en Iraq y Afganistán.

La filtración de estos documentos confidenciales generó gran controversia entre la opinión pública internacional, ya que los cables demostraron que se realizaron miles de asesinatos de civiles, actividades de corrupción, prácticas de tortura, y abusos sobre los cuales el gobierno norteamericano tenía información pero no realizó ninguna acción para intentar detenerlos.

Estos cables también evidenciaron operaciones secretas emprendidas tanto por los militares norteamericanos como por la unidad de fuerzas especiales secreta encargada de detener a los líderes talibanes, ya sea capturándolos o matándolos sin un juicio previo. Así como la utilización de aviones no tripulados (drones) para cazar a talibanes desde su base militares en Nevada, Estados Unidos[221]. También permitieron contar con evidencia de que los grupos talibanes contaban con poderosos misiles tierra-aire que detectaban calor.

Detallaron que la CIA está expandiendo sus operaciones paramilitares dentro de Afganistán, ordenando ataques aéreos, emboscadas y ha financiado a las agencias de espionaje y acciones paramilitares en Afganistán[222], demostrando más irregularidades en las actividades emprendidas por el gobierno

---

[221]Cita textual en ingles: *"the coalition is increasingly using deadly Reaper drones to hunt and kill Taliban targets by remote control from a base in Nevada".* Nick Davies, *Afghanistan war logs: Masive leak of secret files exposes truth of occupation*, [en línea], The Guardian, 25 de Julio 2010, Dirección URL:http://www.theguardian.com/world/2010/jul/25/afghanistan-war-logs-military-leaks, [Consultado el 29 de marzo de 2014].

[222] Cita textual en ingles: "*The Central Intelligence Agency has expanded paramilitary operations inside Afghanistan. The units launch ambushes, order airstrikes and conduct night raids. From 2001 to 2008, the C.I.A. paid the budget of Afghanistan's spy agency and ran it as a virtual subsidiary".* C. J. Chivers; *et.al., View is bleaker than official portrayal of War in Afghanistan*, [en línea], The New York Times, 25 de Julio de 2010, Dirección URL: http://www.nytimes.com/2010/07/26/world/asia/26warlogs.html, [Consultado el 29 de marzo de 2014].

estadounidense como medida para mantener una constante vigilancia del territorio en cuestión.

Señalaron la existencia de abusos por parte de la policía iraquí, ya que realizaban torturas sobre sus prisioneros, problemas de corrupción, brutalidad, extorsión y secuestro dentro de la policía afgana. Todo ello a pesar de que el Pentágono ha invertido mucho dinero en entrenar a fuerzas afganas y restaurar la paz en el país. Este proceso no ha funcionado porque la policía es el sector más corruptible y objeto de desconfianzas por la población civil en Afganistán[223]. Muchos oficiales de policía se convirtieron en parte de grupos talibanes, en oposición a su Estado, lo cual demostró que existen dificultades tanto internas como externas para formar alianzas políticas fuertes para reconstruir a las provincias de Afganistán.

Frente a todas las críticas que surgieron tras conocer esta información, Obama se deslindó de las responsabilidades, argumentando que estas acciones se habían dado durante la administración de su antecesor, el ex presidente George W. Bush, así que no podía hacerse responsable sobre estas decisiones, pero disminuyó sus efectivos militares en el país como muestra de buena voluntad.

Las revelaciones sobre la situación de Afganistán sirvieron también para que algunas organizaciones no gubernamentales de derechos humanos como Amnistía Internacional, cuestionaran no sólo las violaciones a derechos humanos, ya que operan como indicadores de torturas y asesinatos en el país, pero también evidenciaron que la filtración de estos documentos podría afectar sus actividades, argumentando que dar a conocer información sobre las fuentes con las que trabajaban, puede ponerlos en riesgo y dificultar su labor. Sin embargo, es preciso

---

[223] Cita textual en ingles: "*The Pentagon is spending billions to train the Afghan forces to secure the country. But the police have proved to be an especially risky investment and are often described as distrusted, even loathed, by Afghan civilians".* C. J. Chivers; *et.al*., Op.cit., Dirección URL: http://www.nytimes.com/2010/07/26/world/asia/26warlogs.html, [Consultado el 29 de marzo de 2014].

mencionar que hasta el momento no existe ninguna evidencia de un caso en el que se demuestre que la liberación de esta información los haya afectado[224].

4.1.3 China

En el caso de China las revelaciones de Wikileaks proporcionaron información sobre la sospecha de que los ataques cibernéticos de 2005 que afectaron a diversos países se originaron en este país. Al mismo tiempo, puso en discusión las estrictas políticas de restricción dentro de Internet instrumentadas por el gobierno, al impedir el acceso a artículos críticos en contra de su gobierno[225], censura que fue implementada bajo la premisa de restringir el acceso a algunos sitios, para de esta manera poder proteger el poder del Estado, la unidad nacional y los intereses nacionales de China. Además se demuestra la existencia de censura del Partido Comunista Chino a los medios de comunicación y a la información que circula en Internet, quienes solo pueden dar a conocer noticias optimistas y en favor de este gobierno[226], evidenciando que los medios deben adaptarse a las reglas impuestas por ellos.

Se hace referencia a la opinión de los diplomáticos estadounidenses sobre el perfil de Xi Jinping vicepresidente de China, al cual consideran bastante pragmático y realista. Actúa basado no en posturas ideológicas, sino en su ambición, espíritu de autoprotección y posturas elitistas, que se encuentra al frente de un partido

---

[224] Mark Fenster, *Disclosure's Effects: WikiLeaks and Transparency,* [en línea], Revista Iowa Law Review, Universidad de Iowa, Vol. 97:753, 2012, p. 790, Dirección URL:http://www.uiowa.edu/~ilr/issues/ILR_97-3_Fenster.pdf, [Consultado el 29 de marzo de 2014].

[225] Cita textual en ingles: *"recently discovered that Google's worldwide site is uncensored" after he "allegedly entered his own name and found results critical of him".* Dan Sabbagh, *WikiLeaks cables blame Chinese government for Google hacking*, [en línea], The Guardian, 4 de diciembre 2010, Dirección URL:http://www.theguardian.com/technology/2010/dec/04/wikileaks-cables-google-china-hacking, [Consultado el 29 de marzo de 2014].

[226]Cita textual en ingles: "*China's domestic media took to heart Party guidance that news coverage remain upbeat and that negative stories should be avoided (…) Internet controls were extremely tight."* Cable 07BEIJING7035, Embajada de Beijing, Open but not transparent: Local reporters criticize 17th Party Congress Media Strategy, CONFIDENTIAL, Dirección URL: http://internacional.elpais.com/internacional/2010/12/04/actualidad/1291417211_850215.html, [Consultado el 30 de marzo de 2014].

comunista con entrega, que considera que es la clave de una estabilidad social y fuerza nacional perdurable[227], demostrando el interés de Estados Unidos sobre el gabinete de chino, sus posturas políticas, forma de trabajar y de definir estrategias.

En política exterior los cables mostraron que China en realidad apoyaba a Corea del Sur frente a la disputa con Corea del Norte, contrario al discurso presente en los medios de comunicación, poniendo en evidencia el interés de China en generar una nueva geopolítica en sus zonas cercanas. Consideran que una reunificación de Corea podría significar grandes ventajas de comercio para China. Las razones de esta posición es que un sector dentro del gobierno chino consideraba que Corea del Norte ya no es un aliado útil y fiable para ellos y por tal razón no están dispuestos a arriesgarse en un nuevo conflicto armado en la península de Corea[228].

Desconfía de Corea del Norte pero aceptan que por ser su vecino tienen que mantener una relación con el país, a pesar de que en varias ocasiones han intentado romper la relación de China con Estados Unidos[229]. No están de

---

[227]Cita textual en ingles: *"Xi is supremely pragmatic and a realist, driven not by ideology but by a combination of ambition and "self-protection." Xi is a true "elitist" at heart, (…) believing that rule by a dedicated and committed Communist Party leadership is the key to enduring social stability and national strength"* Cable 09BEIJING3128, Embajada de Beijing, Portrait of Vice President Xi Jinping: "Ambitious Survivor" of the Cultural Revolution, 16 de noviembre de 2011, Dirección URL: http://internacional.elpais.com/internacional/2010/12/28/actualidad/1293490818_850215.html, [Consultado el 29 de marzo de 2014].

[228]Cita textual en ingles: *"younger generation Chinese Communist party leaders no longer regarded North Korea as a useful or reliable ally and would not risk renewed armed conflict on the peninsula, according to a secret cable to Washington".* Simon Tisdall, *Wikileaks cables reveal China 'ready to abandon North Korea'*, [en línea], The Guardian, 29 de noviembre 2010, Dirección URL:http://www.theguardian.com/world/2010/nov/29/wikileaks-cables-china-reunified-korea, [Consultado el 31 de marzo de 2014].

[229]Cita textual en ingles: *"He noted that North Korea often tried to play China off the United States, refusing to convey information about U.S.-DPRK bilateral conversations".* Cable 09BEIJING2963, Embajada Beijing, Deputy Secretary Steinberg's meeting with vice foreing minister He Yafei, 26 de septiembre de 2009, SECRET, Dirección URL:

acuerdo con las posturas adoptadas por el gobierno de Corea del Norte para llamar la atención de Estados Unidos, al considerar que estaba tomando una postura muy infantil[230].

Las revelaciones de los cables relacionadas con China no generaron tensiones diplomáticas. Sin embargo, debido a las políticas de censura informática implementadas por el gobierno chino, se bloquearon los enlaces cibernéticos al sitio de Wikileaks. Probablemente la decisión obedeció al temor de que esta información pudiera generar tensiones con Corea del Norte, país que aparece en muchos de los informes diplomáticos[231].

4.2.4 Corea del Norte

Los cables sobre Corea del Norte nos dan una explicación sobre la posición de Estados Unidos frente a Corea del Norte, la cual argumentaba estaba apoyando a Irán en materia de armas nucleares y que su programa nuclear los ha llevado a establecer cooperación con Siria.

Hay cables que hacen referencia a la posible trasferencia de tecnología nuclear entre Corea del Norte e Irán que va en contra de a las resoluciones del Consejo de Seguridad de la ONU, lo cual demuestra el fracaso de China para instrumentar las

---

http://internacional.elpais.com/internacional/2010/11/29/actualidad/1290985223_850215.html, [Consultado el 25 de marzo de 2014].

[230]Cita textual en ingles: *"North Korea wanted to engage directly with the United States and was therefore acting like a 'spoiled child' in order to get the attention of the 'adult'. China encouraged the United States, 'after some time', to start to re-engage the DPRK".* Ibid. Dirección URL: http://internacional.elpais.com/internacional/2010/11/29/actualidad/1290985223_850215.html,

[231]s/a, *Filtración de documentos diplomáticos de los Estados Unidos*, [en línea], Golden Map, Dirección URL: http://es.goldenmap.com/Filtraci%C3%B3n_de_documentos_diplom%C3%A1ticos_de_los_Estados_Unidos#Censura_y_prohibici.C3.B3n_de_WikiLeaks_en_Estados_Unidos.2C_China_y_Francia, [Consultado el 31 de marzo de 2014].

resoluciones de la ONU[232], que ellos mismos habían apoyado, lo cual generó gran preocupación entre los embajadores estadounidenses, ya que esto significaba que se estaban violando resoluciones implementadas por la ONU en materia de armas nucleares.

También se demuestra que Corea del Sur se encuentra preocupada porque China no ha realizado ninguna acción en contra de los programas nucleares de Corea del Norte, ya que consideran que un colapso de ese país desembocaría en una avalancha de refugiados norcoreanos que intentarían dirigirse hacia China lo cual no les conviene. Esto desde la perspectiva de Corea del Sur, es interpretado como un indicador de apoyo hacia Corea del Norte, lo cual hace pensar que se tienen conflictos de interés con China[233].

Estos cables no generaron fricciones diplomáticas, simplemente evidenciaron que Estados Unidos está interesado en saber cuál es la situación de Corea del Norte, pero estos cables tampoco trajeron consecuencias importantes a nivel interno. Sin embargo, el caso se mencionó en esta investigación por la importancia geopolítica que tiene para Estados Unidos este territorio y sus alianzas en materia nuclear con Irán y Siria.

---

[232]Cita textual en ingles: "Information to China regarding transfers of sensitive technologies between Iran and North Korea banned under UN Security Council resolutions provides damning evidence of China's failure to implement UN resolutions it helped craft". Markey Daniel S., *Will Wikileaks hobble U.S. Diplomacy?,* [en línea], Council on Foreing Relations, 1 de diciembre 2010, Dirección URL:http://www.cfr.org/diplomacy-and-statecraft/wikileaks-hobble-us-diplomacy/p23526, [Consultado el 1 de abril de 2014].

[233]Cita textual en ingles: "*The cables also reveal that the South Koreans see their strategic interests in direct conflict with China's creating potentially huge diplomatic over the future of the Korean Peninsula. The South Koreans complain bitterly that China is content with the status quo of a nuclear North Korea, because they fear that a collapse would unleash a flood of North Korean refugees over the Chinese border".* David E. Sanger, *North Korea Keeps the World Guessing*, [en línea], Estados Unidos, New York Times, 29 de noviembre 2010, Dirección URL: http://www.nytimes.com/2010/11/30/world/asia/30korea.html?pagewanted=all, [Consultado el 1 de abril de 2014].

4.2.5 Alemania

Los cables sobre Alemania hacen referencia a las tensiones entre Alemania y Francia por la batalla en materia de tecnología satelital, "revelan que funcionarios alemanes negociaron con Estados Unidos para que éste aceptara ser su socio en el desarrollo del sistema, al mismo tiempo que Francia hacía lo posible por evitar que se unieran"[234]. Generando también controversias internacionales al considerar que este programa podría tener usos tanto comerciales como de inteligencia, lo que significaba la creación de una alianza entre Estados Unidos y Alemania en materia de espionaje[235]. Esto podría significar una gran amenaza a la privacidad internacional, ya que brindaría la posibilidad de ampliar su espectro de espionaje.

En materia de política exterior un cable del embajador estadounidense, Philip Murphy de enero de 2010, aconseja adoptar medidas de "sabotaje encubierto" en las instalaciones clandestinas nucleares de Irán en vez de realizar maniobras militares invasivas que traerían efectos devastadores[236], lo cual demuestran la gran preocupación de Estados Unidos por la situación nuclear de Irán.

También existen cables que hablan de la opinión personal del embajador estadounidense en Alemania, sobre la Canciller Ángela Merkel, su forma de gobernar y su personalidad. La describen como una persona con aversión al riesgo, sin creatividad, insegura en sus relaciones con el gobierno de los Estados

---

[234]Tim Lister, *WikiLeaks revela disputa entre Francia y Alemania por tecnología satelital*, [en línea], CNN México, 3 de enero 2011, Dirección URL: http://mexico.cnn.com/mundo/2011/01/03/wikileaks-revela-disputa-entre-francia-y-alemania-por-tecnologia-satelital, [Consultado el 2 de abril de 2014].

[235] AP, *Wikileaks: Alemania y EEUU planean programa de espionaje satelital,* [en línea], La tercera.com, 3 de enero de 2011, Dirección URL:http://www.latercera.com/noticia/mundo/2011/01/678-335275-9-wikileaks-alemania-y-eeuu-planean-programa-de-espionaje-satelital.shtml, [Consultado el 2 de abril de 2014].

[236]Cita textual en ingles: "*covert sabotage (unexplained explosions, accidents, computer hacking etc) would be more effective than a military strike, whose effects in the region could be devastating".* Josh Halliday, *WikiLeaks: US advised to sabotage Iran nuclear sites by German thinktank*, [en línea], The Guardian, 18 de enero de 2010, Dirección URL:http://www.theguardian.com/world/2011/jan/18/wikileaks-us-embassy-cable-iran-nuclear, [Consultado el 4 de abril de 2014].

Unidos, apodándola "Ángela 'Teflón' Merkel" por considerar que siempre se mantiene alejada de los conflictos[237].

De igual manera hay cables en lo que los diplomáticos norteamericanos hablan de la personalidad del Ministro de Asuntos Exteriores alemán Guido Westerwelle, al cual describen como una "personalidad exuberante", intentando siempre mantener el culto de su personalidad, además de arrogante, con poca experiencia en materia de política exterior y con una visión ambivalente hace la relación con Estados Unidos[238].

El gobierno alemán mostró su inconformidad por la revelación de información confidencial. Un ejemplo de ello fueron las declaraciones del Ministro de Interior de Alemania, Thomas de Maizière, quien declaró que confidencialidad y trasparencia no son excluyentes sino son parte de lo mismo[239]. Es decir, la principal crítica del gobierno alemán fue la falta de pericia del gobierno norteamericano en evitar la divulgación de información y en no mantener los acuerdos de privacidad en las conversaciones.

A pesas de que se dieron varios signos de inconformidad frente a estos documentos, las filtraciones hechas por Wikileaks no afectaron las relaciones

---

[237]Cita textual en ingles: *"Merkel is called "risk averse and rarely creative"; (…) describes Merkel as "insecure" in her dealings with the new U.S. government (…) the Chancellor is given the undiplomatic nickname of "Angela 'Teflon' Merkel" for her habit of steering clear of conflict".* Tristana Moore, *German-U.S. Relations Will Survive WikiLeaks — but the Trust Is Gone*, [en línea], Time World, 29 de noviembre 2010, Dirección URL: http://content.time.com/time/world/article/0,8599,2033526,00.html, [Consultado el 4 de abril de 2014].

[238]Cita textual en ingles: *"little foreign policy experience and an ambivalent view toward the U.S. "There was a consensus among desk officers that Westerwelle was arrogant and too fixated on maintaining his 'cult of personality' ".* Brian Rohan, *U.S. sees top German diplomat arrogant: Wikileaks*, [en línea], Reuters, 28 de noviembre 2010, Dirección URL: http://www.reuters.com/article/2010/11/28/us-germany-wikileaks-idUSTRE6AR3EC20101128, [Consultado el 5 de abril de 2014].

[239]Cita textual en ingles: *"confidentiality and trasparency are not mutually exclusive, but rather two sides of the same coin*".Stark Holger & Rosenbach Marcel, *WikiLeaks Is Annoying, But Not a Threat,* [en línea], Spiegel Online, 20.12.2010 en Päivikki Karhula, What is the effect of Wikileaks for Freedom of Information?, IFLA, Dirección URL:http://www.ifla.org/publications/what-is-the-effect-of-wikileaks-for-freedom-of-information, [Consultado el 6 de abril de 2014].

diplomáticas entre Berlín y Washington "(…) La relación entre ambos países es robusta, firme y densa, más allá de lo publicado y se basan en una amistad histórica y en unos valores comunes", aseguró Steffen Seibert, portavoz oficial del gobierno alemán en Berlín[240].

Sin embargo, si hubo consecuencias internas frente a las revelaciones como lo demostró el caso Helmut Metzner, jefe de gabinete del Ministro de Relaciones Exteriores alemán Guido Westerwelle, quien fue destituido de su cargo tras aceptar que trasmitía información confidencial a los diplomáticos de Estados Unidos sobre listas de participantes en grupos de trabajo, horarios y conversaciones entre políticos alemanes[241], demostrando que las revelaciones de Wikileaks generaron el despido de algunos políticos tras darse a conocer ante la opinión pública las actividades de ellos en el gobierno[242].

4.2.6 Italia

El caso italiano generó controversia al demostrar que los diplomáticos estadounidenses estaban preocupados por la relación entre los gobiernos de Italia y Rusia, además de evidenciar el declive económico alarmante que estaba sufriendo el país. El Primer Ministro, Silvio Berlusconi, continúa siendo fuente de controversia por sus escándalos personales, pero a pesar de todas estas

---

[240] Notimex Berlín, *Niega Alemania que filtraciones de Wikileaks afecten relación con EU*, [en línea], Crónica.com, 29 de noviembre 2010, Dirección URL:http://www.cronica.com.mx/especial.php?id_nota=546947&id_tema=1434, [Consultado el 6 de abril de 2014].

[241] *Severin Weiland*, *WikiLeaks Cables Fallout: Mole in Germany's FDP Party Comes Forward*, [en línea], Spiegel Online, 2 de diciembre 2010, Dirección URL: http://www.spiegel.de/international/germany/wikileaks-cables-fallout-mole-in-germany-s-fdp-party-comes-forward-a-732579.html, [Consultado el 8 de abril de 2014].

[242] Cita textual en ingles: "*The WikiLeaks revelations have claimed their first political scalp (…) the sacking of the German foreign minister's chief of staff, who acted as a mole for the Americans, keeping the US embassy in Berlin posted last year on the confidential negotiations to form Angela Merkel's new government."* Ian Traynor, *WikiLeaks cables claim first scalp as German minister's aide is sacked*, [en línea], The guardian, 3 de diciembre 2010, Dirección URL: http://www.theguardian.com/media/2010/dec/03/wikileaks-first-scalp-german-aide, [Consultado el 6 de abril de 2014].

revelaciones como veremos más adelante, no se generaron tensiones diplomáticas significativas.

Uno de los cables enviado por el entonces embajador en Italia, Ronald P. Spogli, hace mención de la importancia que tiene para Estados Unidos mantener una buena relación con Italia, al ser uno de los pilares de la relación de norteamericana con Europa y ser aliado estratégico, a pesar de que existe falta de liderazgo y de una visión estratégica, lo cual se ha demostrado en la incapacidad del gobierno italiano de hacer frente a muchos de los problemas que aquejan a este país, dando la impresión de que mantienen políticas ineficientes e irresponsables[243].

Se hace también alusión a la forma de gobernar del Primer Ministro de Italia Silvio Berlusconi. Se destacan sus constantes errores y descuidos verbales gracias a la mala elección de palabras, que han llegado a ofender a muchos líderes. Adicionalmente su subraya su predilección por los asuntos personales antes que de los estatales. Se argumenta que utiliza su posición para obtener ventaja frente a sus adversarios políticos, lo cual ha dañado la reputación de Italia en Europa y ha llegado a ser considerado como una broma.[244]

Por otra parte, los *Cablegates* destacaron que los diplomáticos estadounidenses se encontraban preocupados por la estrecha relación entre el Primer Ministro de

---

[243]Cita textual en ingles: *"Its leadership frequently lacks strategic vision (...) or as properly-developed as one would expect for a modern European country. Italian leaders' unwillingness and inability to address many of the chronic problems that plague their society (…) have caused concern among Italy's partners and given the impression of feckless and inefficient governance."* Cable 09ROME128, Embajada de Roma, Final thoughts on the U.S.-Italy relationship: What we can ask from a strong ally, 5 de febrero de 2009, Confidencial, Dirección URL: http://www.cablegatesearch.net/cable.php?id=09ROME128, [Consultado el 5 de abril de 2014].

[244]Cita textual en ingles: "*His frequent verbal gaffes and poor choice of words have offended nearly every demographic in Italy and many EU leaders. His perceived willingness to put personal interests above those of the state, his preference for short-term solutions over long-term investment, and his frequent use of public institutions and resources to gain electoral advantage over his political adversaries has harmed Italy's reputation in Europe and has provided an unfortunately comic tone to Italy's reputation".* Cable 09ROME128, Embajada de Roma, Final thoughts on the U.S.-Italy relationship: What we can ask from a strong ally, 5 de febrero de 2009, Confidencial, Dirección URL: http://www.cablegatesearch.net/cable.php?id=09ROME128, [Consultado el 9 de abril de 2014].

Italia, Silvio Berlusconi y el Primer Ministro de Rusia, Vladimir V. Putin quienes en repetidas ocasiones han intercambiado regalos lujosos, contratos en materia de energía muy lucrativos y constantes comunicaciones, mediante un sospechoso intermediario italiano[245].

Se demuestra esta estrecha relación con otros cables donde Berlusconi argumenta que Vladimir Putin es un amigo íntimo al cual admira por su estilo de gobierno autoritario y decisivo, el cual es considerado como similar al suyo y por tal razón mantiene mayor comunicación que con cualquier otro líder mundial[246]. Esta alianza no solo representaba una amenaza para los intereses de Estados Unidos en Europa, sino que el gobierno estadounidense considera que podría convertirse en un problema en caso de que se establezcan acuerdos en materia energética, tema de gran relevancia para las relaciones entre Rusia e Italia[247].

La revelación que causó controversia fue la dada a conocer por el embajador de Estados Unidos en Roma, David Thorne, quien hablaba sobre los escándalos sexuales, las investigaciones criminales, problemas familiares y financieros del Primer Ministro Silvio Berlusconi, los cuales han comenzado a afectar su salud personal y política[248]. Demuestran sus supuestos vínculos con la mafia italiana, su

---

[245]Cita textual en ingles: *"an extraordinarily close relationship between Vladimir V. Putin the Russian prime minister, and Silvio Berlusconi, the Italian prime minister and business magnate, including "lavish gifts", lucrative energy contracts and a "shadowy" Russian-speaking Italian go-between". Vease:* Giles Watson, *Wikileaks Reveals Berlusconi as "Feckless", "Ineffective" and "Mouthpiece of Putin",* en línea], Italian Life, 29 de noviembre 2010, Dirección URL:http://www.corriere.it/International/english/articoli/2010/11/29/wikileaks-Berlusconi-leader.shtml, [Consultado el 10 de abril de 2014].

[246]Cita textual en ingles: "Berlusconi believes that Putin is his close and personal friend and continues to have more contact with Putin than with any other world leader (…) Berlusconi admires Putin's macho, decisive, and authoritarian governing style, which the Italian PM believes matches his own". Cables 09ROME97, Embajada de Roma, Italy-Russia relations: The view from Rome, 26 de enero de 2009, SECRETO, Dirección URL: http://www.cablegatesearch.net/cable.php?id=09ROME97, [Consultado el 9 de abril de 2014].

[247]Cita textual en ingles: *"In its relationship with Russia, energy is the most important bilateral issue and the quest for stable energy supplies from Russia frequently forces Italy to compromise on security and political issues"* Cables 09ROME97, Embajada de Roma, Italy-Russia relations: The view from Rome.

modo de vida alocado, que se han convertido en un espectáculo público, lo cual ha dañado la reputación del Primer Ministro italiano en los últimos años[249].

Los diplomáticos estadounidenses también demostraron que contaban con información delicada sobre las tres principales mafias italianas y le informaron al gobierno de los Estados Unidos, para convencer al gobierno italiano sobre el grave peligro que representaba el crimen organizado alojado dentro de su territorio. El crimen organizado no sólo es visto como riesgo para el país sino para toda Europa, particularmente porque apoya el terrorismo en Colombia y Asia Central, a través del tráfico de drogas y violación a derechos de propiedad intelectual. Lo que supone una fuente de desestabilización política para cualquier gobierno[250]. Hacen recomendaciones de las acciones multifacéticas que se podrían tomar para combatir a estas mafias, las cuales se operarían a través de la Secretaría de Estado. Esta información fue de gran trascendencia, ya que evidenció que los Estados Unidos estaban intentando dirigir el funcionamiento del gobierno italiano, violando su soberanía.

---

[248]Cita textual en ingles: *"Sex scandals, criminal investigations, family problems and financial concerns appear to be weighing heavily on Berlusconi's personal and political health, as well as on his decision-making ability".* Cable 09ROME1187, Embajada de Roma, Italy: Scandals taking toll on Berlusconi's personal and political health, 27 octubre 2009, Confidencial, Dirección URL:http://www.cablegatesearch.net/cable.php?id=09ROME1187, [Consultado el 11 de abril de 2014].

[249]Cita textual en ingles: *"Berlusconi's frequent late nights and penchant for partying hard mean he does not get sufficient rest.(…) alermo-based mafia investigation involving another longtime Berlusconi ally and confidant already convicted of ties to organized crime could turn into a damaging public spectacle".* Cable 09ROME1187, Embajada de Roma, Italy: Scandals taking toll on Berlusconi's personal and political health, 27 octubre 2009, Confidencial, Dirección URL:http://www.cablegatesearch.net/cable.php?id=09ROME1187, [Consultado el 11 de abril de 2014].

[250] Cita textual en ingles: *"The Italian crime syndicates help support terrorist groups in Colombia and Central Asia through drug trafficking; violate the intellectual property rights of American businesses and artists; (..) pose potential public health risks to U.S. military and dependents stationed in southern Italy."* Cable 08NAPLES118, Consulado de Nápoles, Organized Crime III: Confronting Organized Crime in Southern Italy, 6 de junio 2008, Dirección URL:http://internacional. elpais.com/internacional/2011/01/07/actualidad/1294354804_850215.html, [Consultado el 11 de abril de 2014].

Sin embargo, no hubo efectos diplomáticos. Las únicas consecuencias que trajeron estos cables fueron el rechazo por parte del ministro de Asuntos Exteriores italiano, Franco Frattini, quien en varios cables afirmó que Julian Assange pretendía destruir al mundo con estas filtraciones y que la revelación de los *Cablegates* podría llamarse el 11 de septiembre de la Diplomacia Internacional[251].

La declaración del Ministro de Asuntos Exteriores italiano no fue tomado como un posicionamiento presidencial, ya que el Primer Ministro Silvio Berlusconi proclamó que el caso estaba cerrado, después de una disculpa por parte de Hillary Clinton en el que consideraba que "Berlusconi es el mejor amigo de América" (EE.UU).

Estas revelaciones no generaron graves tensiones a nivel exterior, pero si hubo reacciones en el interior, ya que el líder de la oposición italiana Dario Franceschini se pronunció a favor de que el Primer Ministro Silvio Berlusconi se presentara ante el Parlamento para explicar ante el público la información que aparece de manera detallada en los cables diplomáticos[252], incrementando las tensiones e inconformidades con el gobierno en turno.

4.2.7 México

Destacaron los comentario enviados por el entonces Embajador de Estados Unidos en México Carlos Pascual, quien hacen referencia al audaz plan de reformas estructurales anunciadas por el presidente Felipe Calderón, cuya instrumentación se podría dificultar por la caída de su popularidad entre la

---

[251]Cita textual en ingles: "*Franco Frattini, Italy's current foreign affairs minister, who loudly proclaimed that the WikiLeaks revelations were the "9/11 of International Diplomacy" and that Julian Assange wants "to destroy the world".*"Annalisa Piras, *Wikileaks cables portrait of Silvio Berlusconi is a worry beyond Italy*, [en línea], The Guardian, 3 de diciembre 2010, Dirección URL: http://www.theguardian.com/commentisfree/2010/dec/03/wikileaks-cables-silvio-berlusconi, [Consultado el 13 de abril de 2014].

[252] Annalisa Piras, *Wikileaks cables portrait of Silvio Berlusconi is a worry beyond Italy*, [en línea], The Guardian, 3 de diciembre 2010, Dirección URL: http://www.theguardian.com/commentisfree/2010/dec/03/wikileaks-cables-silvio-berlusconi, [Consultado el 13 de abril de 2014].

población mexicana, debido a los problemas de inseguridad que vive el país[253]. También se hace referencia que el PAN perdió la mayoría electoral en las elecciones del 2009, mostrando que el entonces presidente Calderón no contaba con el respaldo esperado y que sus acciones tampoco tenían total credibilidad.

Con las revelaciones de Wikileaks se tuvo acceso a los cables en los que el embajador Carlos Pascual cuestionaba la estrategia gubernamental de México en materia de seguridad y la guerra contra el narcotráfico. "Califican al Ejército mexicano de incapaz, con aversión al riesgo, inepto como policía; con descoordinación en los cuerpos de seguridad; con carencia de inteligencia; y adoctrinamiento del Ejército pretextando modernización, impulsó a una guerra interna y a servir a misiones extranjeras; las fuerzas armadas prácticamente sometidas al mando estadounidense; solicitudes de apoyo por funcionarios mexicanos desesperados y reconocimiento de pérdida de control de partes del territorio y corrupción generalizada"[254]. Evidenciando la situación de corrupción, una gran descoordinación entre las agencias de seguridad, que ha dificultado el manejo de las instituciones de seguridad, llevando a una competencia de suma cero en donde el éxito en materia de seguridad por parte de alguna de las instituciones es vista por el resto como un fracaso, lo que ha llevado a no lograr establecer operaciones conjuntas entre estas instituciones. Señalan el riesgo de que esto puede llevar a convertir a México en un estado fallido, por lo que necesita la contención de las organizaciones criminales, ya que ello significaría que el

---

[253]Cita textual en ingles: "*Calderon's bold plan for ten ambitious areas for reform, announced in September, has yet to translate into any concrete initiatives. His personal popularity numbers while over fifty percent and historically in line with his predecessors, have dropped ten points since last February, the lowest level of support during his first three years in office. Even more worrying is an eight point drop in his approval on the security front, an issue on which he has garnered his strongest support*". Cable 09MEXICO3423, Embajada de Estados Unidos en México, Las perspectivas del PAN son sombrías: Pascual, 4 de diciembre 2009, Dirección URL: http://wikileaks.jornada.com.mx/cables/gobierno-felipe-calderon/sugieren-a-valenzuela-pedir-a-mexico-que-respalde-sin-ambiguedades-la-politica-estadunidense-para-honduras-cable-09mexico3423/#sthash.F0YY8XTn.dpuf, [Consultado el 16 de abril de 2014].

[254]Manuel Bartlett, *Sumisión intolerable*, [en línea], México, El Universal, 16 de diciembre 2010, Dirección URL:http://hitucomolaveis.wordpress.com/page/61/, [Consultado el 15 de abril de 2014].

sistema federal mexicano se viera socavado significativamente si continúan con la presencia de los cárteles de la droga en la periferia del país[255].

Los cables también mostraron el interés del gobierno norteamericano en las administraciones de Felipe Calderón y de Vicente Fox, en su personalidad así como perfil psicológico y forma de gobernar, parecía que buscaba conocer mejor a los gobernantes de México, para contar con información estratégica de sus adversarios de gran utilidad en el momento de establecer negociaciones.

Las declaraciones del entonces embajador de Estados Unidos en México trajeron como consecuencia que el ex Presidente Felipe Calderón solicitara el despido del Embajador Carlos Pascual[256], quien se vio obligado a dimitir su cargo[257]. Es decir, estas revelaciones generaron mayor tensión en las relaciones bilaterales entre México y Estados Unidos, ya que las fuertes críticas a las acciones emprendidas en material de seguridad y lucha contra el narcotráfico durante la gestión del presidente Felipe Calderón contrastaban con el discurso oficial del gobierno norteamericano que reconocía públicamente los esfuerzos mexicanos en la materia.

---

[255] Cita textual en ingles: "*Clearly Mexico is not an impending failed state, (…), but there are serious consequences of failure if President Calderon does not succeed in containing Mexico's criminal organizations. In all likelihood, Mexico's federal system would be significantly undermined should the cartels retain and strengthen their presence in Mexico's periphery."* Cable 09MEXICO1055, Embajada de Estados Unidos en México, *Serias consecuencias, si Calderón no logra contener el crimen,* 14 de abril 2009, Dirección URL:http://wikileaks.jornada.com.mx/cables/gobierno-felipe-calderon/09mexico1055/#sthash.kbQWQ5GP.dpuf, [Consultado el 13 de abril de 2014].

[256] Carlos Pascual asumió el cargo de Embajador en México en agosto de 2009. Anteriormente fue embajador de Estados Unidos en Ucrania de 2000 a 2003 y Coordinador para Reconstrucción y Estabilización en el Departamento de Estado. Graduado de Harvard y Stanford. Renunció a su puesto en marzo de 2011 y fue remplazado por Anthony Wayne. Véase: *Perfil Carlos Pascual, de Stanford y de Harvard a México*, [en línea], México, El Universal, 26 de marzo de 2009, Dirección URL:http://www.eluniversal.com.mx/notas/586468.html, [Consultado el 15 de abril de 2014].

[257]Cita textual en ingles: *"The U.S. ambassador to Mexico was forced to resign after the release of cables in which he criticized the Mexican government's efforts to fight drug trafficking"* Jose de Cordoba, *U.S. Ambassador to Mexico Resigns Following WikiLeak Flap*, WALL ST. J. (Mar. 19, 2011), http://online.wsj.com/article/SB10001424052748704021504576211282_543444242.html en Mark Fenster, Disclosure's Effects: WikiLeaks and Transparency, [en línea], Revista Iowa Law Review, Universidad de Iowa, Vol. 97:753, 2012, Pp. 793-794, Dirección URL:http://www.uiowa.edu/~ilr/issues/ILR_97-3_Fenster.pdf, [Consultado el 20 de abril de 2014].

Sin embargo, la opinión pública criticó el hecho de que no se realizaran proclamaciones más severas por parte de la Secretaría de Relaciones Exteriores sobre la política de intervención. Las entrevistas gubernamentales estuvieron centradas en la organización (Wikileaks) encargada de las filtraciones, pero no hubo pronunciamientos en contra de las acciones cometidas por el gobierno de los Estados Unidos, que violaron la soberanía nacional, sino que las relaciones bilaterales continuaron sin cambios. Esto lo podemos observar en la siguiente cita: "La respuesta del gobierno mexicano a estas descalificaciones, señalamientos de enajenación de soberanía, de impotencia del Estado, fue aceptar sumisamente el dictado estadounidense: "reprobación categórica de la revelación ilegal de documentos imputados a la diplomacia estadounidense, no reflejan el posicionamiento de Estados Unidos" (SRE)"[258]. Es decir, Wikileaks significó el cambio del embajador norteamericano en México, pero no llevó a radicalizar el discurso del gobierno mexicano frente a la información dada a conocer sobre las administraciones panistas y tampoco se puso a discusión la política de intervención de los Estados Unidos, por el contrario el gobierno mexicano optó por convertirse en un aliado de Estados Unidos al considerar que estas filtraciones eran ilegales y repudiar también a la organización y a su fundador.

4.2.8 Argentina

En el caso de Argentina podemos observar que no existieron consecuencias diplomáticas evidentes, aunque la información que revelaron los cables fue considerada por la opinión pública argentina como importante y esperaban que el gobierno norteamericano brindara una explicación sobre las opiniones ahí plasmadas. Sin embargo, esto no sucedió y la embajada de Estados Unidos en Buenos Aires solamente respondió como explicación que "los cables diplomáticos reflejaban el análisis interno diario y apreciaciones directas que hacen a las

[258]*Manuel Bartlett, Sumisión intolerable,* [en línea], *El Universal, 16 de diciembre de 2010,* Dirección URL: http://www.eluniversal.com.mx/editoriales/50993.html, [Consultado el 18 de abril de 2014].

deliberaciones sobre las relaciones externas del gobierno (…) contienen expresiones preliminares e incompletas relacionadas con asuntos de política exterior"[259]. Es decir, no daban ninguna explicación sobre las razones para obtener conversaciones sobre las políticas y acciones de los presidentes en turno, pero también información sobre su carácter y personalidad, como veremos a continuación.

Uno de los cables enviados por el embajador Lino Gutiérrez hablaba del ahora denominado "Estilo K", refiriéndose a la forma de gobernar personalista y a menudo errático en la toma de decisiones, además de caracterizarse por un enfoque global a corto plazo y de centrarse en el aspecto interno más que en el exterior del entonces presidente Néstor Kirchner, que no daba la posibilidad de ningún tipo de disenso y que aplicaba tácticas para debilitar a la oposición y de esta manera mantener la estabilidad de Argentina, lo que rompe con los esquemas de democracia[260].

Este cable revela un perfil psicológico sobre el presidente en el que se dejar ver que Néstor Kirchner tiene necesidad de mantener siempre el control, por lo que no delegaba tareas, que tomaba decisiones rápidas y mantenía una constante lucha

---

[259] Alejandro Rebossio y Luis Doncel, Las revelaciones de Wikileaks sobre la presidenta Kirchner acaparan el debate político en Argentina, [en línea], Buenos Aires, El País, 30 de noviembre 2010, Dirección URL: http://internacional.elpais.com/internacional/2010/11/30/actualidad/1291071603_850215.html, [Consultado el 17 de abril de 2014].

[260] Cita textual en ingles: "*President Nestor Kirchner's personalistic, often erratic operating and decision-making style defines current Argentine policymaking and is characterized by an overarching focus on the short-term and politically expedient accumulation and maintenance of domestic political power. Kirchner's domestic political style leaves no room for dissent and utilizes divide-and-*conquer tactics to weaken the political opposition."Cable 06BUENOSAIRES1462, Embajada de Estados Unidos en Buenos Aires, Argentina: The K-style of politics, 29 de junio 2006, Dirección URL: http://wikileaks.org/cable/2006/06/06BUENOSAIRES1462.html, [Consultado el 17 de abril de 2014].

contra sus enemigos[261] Lo cual significa que la embajada consideraba que todas las decisiones importantes del país tenía que pasar antes por Kirchner, que en ocasiones tomaba decisiones de manera apresurada y se tomaba de manera muy personal a sus enemigos.

Del mismo modo que ocurrió en el caso mexicano, el Departamento de Estado de los Estados Unidos también se mostró interesado en conocer más sobre la personalidad de la presidente Cristina Fernández de Kirchner, haciendo varias preguntas sobre el manejo de la ansiedad, cómo afecta esto su toma de decisiones, cómo actúa ante situaciones de estrés y si requiere de alguna medicación cuando la sobrepasa el estrés y la ansiedad[262]. Se tenían interrogantes sobre la posibilidad de algún tipo de trastorno bipolar y si compartía la misma visión gubernamental que su esposo o si era más moderada.

Por otra parte, también se generaron tensiones sobre la política exterior adoptada por el gobierno de Argentina y su falta de apego a los protocolos en los siguientes términos: comentarios erráticos con dignatarios extranjeros, asesores sin mucha

---

[261]Cita textual en ingles: *"Kirchner's psychological profile includes a need to always be in control, quick and decisive decision making, and a constant struggle against perceived enemies. Kirchner does not delegate policymaking, making all of the important decisions himself".* Cable 06BUENOSAIRES1462, Embajada de Estados Unidos en Buenos Aires, Argentina: The K-style of politics, junio 2006, Dirección URL: http://wikileaks.org/cable/2006/06/06BUENOSAIRES1462.html, [Consultado el 18 de abril de 2014].

[262]Cita textual en ingles: *"How is Cristina Fernandez de Kirchner managing her nerves and anxiety? How does stress affect her behavior toward advisors and/or her decisionmaking? What steps does Cristina Fernandez de Kirchner or her advisers/handlers, take in helping her deal with stress? Is she taking any medications?".* Cable 09STATE132349, Secretaría de Estado, Argentina: Kirchner interpersonal, 31 de diciembre 2009, Dirección URL:http://www.wikileaks.ch/cable/2009/12/09STATE132349.html, [Consultado el 18 de abril de 2014].

experiencia en el extranjero y el presidente Néstor Kirchner mantiene poco contacto con el Ministerio de Relaciones Exteriores[263].

Otro de los cables hacía referencia a la falta de habilidades del gobierno argentino en materia de política exterior y negociaciones internacionales. Ejemplo de ello fue que en un viaje a El Salvador realizado por Cristina Fernández que resultó infructuoso, se abordó el caso de Honduras en donde su postura regresar al poder al destituido presidente de Honduras, Manuel Zelaya, tras el golpe de Estado[264].

Lo sorprendente de este caso es que a pesar de que las filtraciones revelan información sobre la vida personal y salud de los mandatorios argentinos, la administración de Cristina Kirchner permaneció en silencio, sin dar ninguna declaración ni a favor ni en contra frente a Wikileaks. Fue hasta comienzos de 2011 que se tomaron acciones, pero no fue una respuesta diplomática, sino comercial, como lo demuestra la siguiente cita "material estadounidense que llevó a Buenos Aires un avión militar fuese incautado y para que sus funcionarios lancen una ofensiva fiscal y comercial contra empresas extranjeras y estadounidenses"[265]. Esta acción fue tomada por varios sectores como una respuesta para que Estados Unidos se diera cuenta del descontento que prevalecía por la filtración, pero sin afectar de manera directa las relaciones bilaterales.

---

[263]Cita textual en ingles: "*President Kirchner is not skilled at international diplomacy and often ignores basic protocol. Kirchner's gaffes with foreign dignitaries are legendary (…) No one from the Foreign Ministry is part of Kirchner's inner circle of advisors, and very few of Kirchner's close associates had overseas experience before Kirchner became President".* Cable 06BUENOSAIRES1462, Embajada de Estados Unidos en Buenos Aires, Argentina: The K-style of politics, [Consultado el 20 de abril de 2014].

[264]s/a, *Wikileaks: las diez peores cosas que dijo EE.UU. de Cristina y del Gobierno*, [en línea], MDZ Online, 30 de noviembre 2010, http://www.mdzol.com/nota/255989/, [Consultado el 22 de abril de 2014].

[265] Ana Baron, *Para EE.UU., la relación bilateral está teñida de política interna*, [en línea], El Clarín, Argentina, 6 de marzo de 2011, Dirección URL: http://www.clarin.com/politica/EEUU-relacion-bilateral-politica-interna_0_439156142.html, [Consultado el 22 de abril de 2014].

4.2.9 Ecuador

Uno de los cables que generó más tensiones diplomáticas entre Ecuador y Estados Unidos fue el enviado en julio de 2009 por la entonces embajadora de Estados Unidos en Quito, Heather Hodges, quién hace un detallado relato sobre los actos de corrupción, abuso de poder, obstrucción de investigaciones, etc. cometido por el ex comandante de la política de Ecuador, Jaime Aquino Hurtado Vaca, a quien se acusa de haber usado su cargo como comandante de la Policía Nacional y sus influencias personales para extorsionar dinero y propiedades, malversar fondos públicos, facilitar el tráfico de personas y obstruir investigaciones sobre colegas corruptos[266]. Revelan también que Hurtado Vaca ha podido realizar estas actividades ilegales porque el gobierno de Ecuador tiene una débil supervisión institucional en materia de seguridad nacional, lo cual se traduce en un mínimo riesgo de ser sancionados por cometer actos de corrupción[267], demostrando que esta información no era un secreto, sino que hasta el presidente Correa sabía lo que estaba sucediendo.

Tras la revelación de esta información el gobierno de Rafael Correa expresó "su profunda indignación ante las especulaciones aparecidas en el citado cable"[268] y expulsó a la embajadora Heather Hodges del territorio ecuatoriano y la nombró persona *non grata*, lo cual la llevó a tener que abandonar el país. El gobierno de

---

[266]Cita textual en ingles: *"Jaime Aquilino Hurtado Vaca has used his office as Commander of the National Police and personal influence to extort cash and property, misappropriate public funds, facilitate human trafficking, and obstruct the investigation and prosecution of corrupt colleagues."* Cable 09QUITO572, Embajada de Quito, Visas Donkey- Corruption Visa revocation: Jaime Aquino Hurtado Vaca, 10 de julio de 2009, Secret, Dirección URL: http://www.cablegatesearch.net/cable.php?id=09QUITO572, [Consultado el 21 de abril de 2014].

[267]Cita textual en ingles: *"Ecuador has very weak institutional oversight of its law enforcement agencies (…) Because of these institutional failings, National Police officers face minimal risk of exposure or punishment when they engage in corrupt acts".* Cable 09QUITO572, Embajada de Quito, *op.cit*., [Consultado el 21 de abril de 2014].

[268]s/a, *Ecuador expulsa a la embajadora de EU tras un cable de WikiLeaks,* [en línea], CNN México, 5 de abril de 2011, Dirección URL:http://mexico.cnn.com/mundo/2011/04/05/ecuador-expulsa-a-la-embajadora-de-eu-tras-un-cable-de-wikileaks, [Consultado el 23 de abril de 2014]

Ecuador acusó al gobierno de Estados Unidos de espiar a la policía ecuatoriana y de intentar involucrar al presidente Correa en este caso de corrupción.

Esta acción fue criticada por algunos sectores del propio gobierno ecuatoriano que consideraron que dentro de la diplomacia existían otros medios para externar el descontento sin poner en riesgo las relaciones bilaterales. "La expulsión de la embajadora es una medida muy grave desde el punto de vista diplomático e implica un enfriamiento de las relaciones entre los dos países", señaló el ex vicecanciller Marcelo Fernández de Córdova[269]", teniendo en cuenta que existen temas importantes dentro de la agenda de la relación bilateral entre Estados Unidos y Ecuador, como el acuerdo de preferencia arancelaria.

Podemos hacer referencia a otro cable en el que la embajada critica la relación entre el presidente Rafael Correa y los medios de comunicación comerciales, por Correa considera que estos proteger solamente los intereses de sus propietarios y no representar los intereses de los ciudadanos ecuatorianos[270]. Se enfatiza que desde el comienzo de la administración de Correa han existido fricciones entre el gobierno y las televisoras nacionales, argumentándose que tomó el control de dos televisoras nacionales porque solo buscaban sus intereses personales. Por lo que los diplomáticos generaron alertas por las reformas constitucionales que se pretendían hacer en materia de comunicaciones ya que Correa pretendía establecer el "socialismo del siglo XXI" a través de la creación de un sistema de

---

[269]Paúl Mena Erazo, Ecuador y EE.UU. en nuevo roce bilateral, [en línea], BBC Mundo, 5 de abril 2011, Dirección URL: http://www.bbc.co.uk/mundo/noticias/2011/04/110405_ecuador_eeuu_embajadora_lr.shtml, [Consultado el 10 de agosto de 2014].

[270]Cita textual en ingles: *"Since President Rafael Correa came to office in 2007 he has criticized the Ecuadorian commercial media as "incompetent," and complained that the majority of media outlets were protective of the business interests of their owners and not representative of the interests of Ecuadorian citizens. (…)President Correa's actions and the provisions of the new constitution present a serious challenge to Ecuadorian media and freedom of the press".* Cable 09QUTO108, Commercial media in Ecuador worried about the President and the new constitution, 11 de febrero de 2009, Unclassified, Dirección URL: http://wikileaks.org/cable/2009/02/09QUITO108.html, [Consultado el 23 de abril de 2014].

comunicación social[271]. Mostrando que eran inciertas las consecuencias que podrían traer para la libertad de prensa estas nuevas medidas, ya que planteaban que las televisoras comerciales debían seguir los mandatos presidenciales, lo que no abonaba a favor de libertad de expresión, sino que por el contrario podía coartarla.

También se hace evidente en otro de los cables la grave situación en material de seguridad, por el narcotráfico en la frontera con Colombia, y por la presencia de grupos criminales y terroristas en la frontera norte. Las FARC utiliza este territorio para descanso, asistencia médica, reabastecimiento, adquisición de armas y explosivos, así como procesamiento de cocaína y siembra de otros productos ilegales[272]. Según la embajada no se había logrado controlar esta situación en la frontera con Colombia debido a la falta de recursos, a la corrupción entre policías y militares y a una tensa situación en las relaciones bilaterales de Ecuador con Colombia.

Otro de los cables hace referencia a la relación bipolar entre el gobierno de Correa y los Estados Unidos, donde en algunas ocasiones el gobierno de Correa se pronunciaba a favor de mejorar las relaciones con Estados Unidos y otras ocasiones se manifestaba en oposición. Esta relación cambiante y volátil generaba una respuesta cautelosa por parte de los diplomáticos estadounidenses.

---

[271]Cita textual en ingles "*Ecuador's new constitution reflects President Correa's promise to implement "Socialism of the 21st Century" by creating a "system of social communication," among other provisions."* Cable 09QUTO108, Commercial media in Ecuador worried about the President and the new constitution, 11 de febrero de 2009, Unclassified, Dirección URL: http://wikileaks.org/cable/2009/02/09QUITO108.html, [Consultado el 24 de abril de 2014].

[272]Cita textual en ingles *"Ecuador's greatest counterterrorism and security challenge remained the presence of Colombian narcotics, criminal and terrorist groups in the northern border region (…) FARC, regularly used Ecuadorian territory for rest, medical aid, weapons and explosives procurement, recuperation, resupply, and training, as well as coca processing and limited planting and production".* Cable 09QUITO1218, Embajada de Quito, 21 de diciembre 2009, Unclassified, Dirección URL:http://wikileaks.org/cable/2009/12/09QUITO1218.html#, [Consultado el 23 de abril de 2014].

Finalmente, como consecuencia de los problemas diplomáticas que generaron la filtración de estos cables diplomáticos el gobierno de Rafael Correa se pronunció en 2012 a favor de asilar al Julian Assange dentro de su embajada en Londres y ofrecerle asilo político en Ecuador, lo cual propició mayores tensiones entre los Estados Unidos y Ecuador.

Tabla 6 Comparativo de las consecuencias de los cables diplomáticos de Wikileaks

País	Clasificación	Información Revelada	Consecuencias internas	Consecuencia Diplomáticas
Egipto	Situación de corrupción por parte de las autoridades, violación a derechos humanos e impunidad	• Interés de EUA por mantener la promoción de las negociaciones entre Israel y la Autoridad Palestina • Abusos y brutalidad por parte de policía egipcia • Negativa del gobierno de Mubarak de tratar temas de derechos humanos	Incrementaron el malestar de la población contra el gobierno interno	No generó consecuencias diplomáticas.
Iraq y Afganistán (*War Logs)*	Situación de corrupción por parte de las autoridades, violación a derechos humanos e impunidad	• Actividades de los soldados y del gobierno de los EUA durante las intervenciones militares. • Actividades de corrupción, prácticas de tortura, abusos y muerte de civiles • Utilización de *drones* para cazar a talibanes por EUA	Se cuestionó que el Pentágono gaste tanto dinero para entrenar a fuerzas afganas y restaurar la paz en el país sin resultados fructíferos.	No generó consecuencias diplomáticas. Cuestionamientos ante ONG's por las violaciones a derechos humanos.
China	Situación de corrupción por autoridades, violación a derechos humanos e impunidad. Documentos que hablen de opinión personal de los diplomáticos	• Políticas de restricción dentro de Internet instrumentadas por el gobierno • China apoya a Corea del Sur frente a la disputa con Corea del Norte • Perfil psicológico del vicepresidente de China, Xi Jinping de China	El gobierno chino bloqueo los enlaces al sitio de Wikileaks.	No generó consecuencias diplomáticas

Corea del Norte	Documentos relacionados con cuestiones de seguridad nacional	Corea del Norte apoya a Irán con trasferencia tecnológica nuclear y mantiene cooperación nuclear con Siria	No hubo consecuencias internas.	No generó consecuencias diplomáticas
Alemania	Documentos que hablan sobre la opinión personal de los diplomáticos sobre sus homólogos o de presidentes de otros países	• Planes secretos, personalidad de los principales mandatarios alemanes • Tensiones entre Alemania y Francia por la batalla en materia de tecnología satelital	El jefe de gabinete del Ministro de Relaciones Exteriores fue destituido por trasmitir información confidencial.	Varios signos de inconformidad pero no se afectaron las relaciones diplomáticas entre Berlín y Washington.
Italia	Documentos que hablen sobre la opinión personal de los diplomáticos sobre sus homólogos o de presidentes de otros países. Documentos relacionados con intereses económicos de Estados Unidos en el exterior.	• Preocupación por la relación entre los gobiernos de Italia y Rusia. • Declive económico alarmante a causa de la falta de liderazgo y de una visión estratégica por parte del gobierno italiano • Forma de gobernar del Primer Ministro Silvio Berlusconi, escándalos personales, investigaciones criminales y financieras • Los problemas con la mafia italiana y los carteles de la droga	El líder de la oposición italiana Dario Franceschini pidió que el Primer Ministro Silvio Berlusconi rindiera cuentas ante el Parlamento	No hubo consecuencias diplomáticas.
México	Documentos que hablan sobre la opinión personal de los diplomáticos sobre sus homólogos o de presidentes de otros países. Situación de corrupción por parte de las autoridades, violación a derechos humanos e impunidad.	• Califican al ejército de incapaz, descoordinado, casi sometidos al mando estadounidense; pérdida de control de partes del territorio y corrupción generalizada. • Cuestionamiento de estrategia gubernamental en materia de seguridad y la guerra contra el narcotráfico. • Personalidad y perfil psicológico de los mandatarios.	Indignación ante la opinión pública por la falta de firmeza y respuesta por parte del gobierno frente a los datos dados a conocer.	Despido del entonces embajador de los Estados Unidos, Carlos Pascual. Sin embargo las relaciones bilaterales continuaron sin cambios.

Argentina	Opinión personal de los diplomáticos sobre sus homólogos o de presidentes de otros países. Situación de corrupción por parte de las autoridades, violación a derechos humanos e impunidad.	• Forma de gobernar personalista del presidente Néstor Kirchner y Cristina Fernández de Kirchner • Silenciar a la oposición como forma para mantener la estabilidad de Argentina. • Perfil psicológico de los mandatarios	Tomaron acciones comerciales al incautar un avión estadounidense con mercancía para ofensiva fiscal y comercial.	No hubo consecuencias diplomáticas.
Ecuador	Situación de corrupción por parte de las autoridades, violación a derechos humanos e impunidad. Documentos relacionados con cuestiones de seguridad nacional	• Relato sobre los actos de corrupción, abuso de poder, obstrucción de investigaciones, etc. cometido por el ex comandante de la política, Jaime Hurtado Vaca • Débil supervisión institucional en materia de seguridad nacional • Presencia de grupos criminales y terroristas en la frontera norte de las FARC • Ficciones con las televisoras, intención del presidente de hacer reformas constitucionales en materia de telecomunicaciones.	Opositores al gobierno de Correa consideraron que las medidas diplomáticas adoptadas se extralimitaban. El gobierno de Correa decide asilar al creador de Wikileaks en su embajada de Londres y ofrecerle asilo diplomático en Ecuador.	El presidente Rafael Correa expulsó a la embajadora de EE.UU Heather Hodges del territorio ecuatoriano y la nombró persona non grata. Acusó al gobierno de EE.UU de espiar sobre asuntos de soberanía nacional y de involucrar al presidente en caso de corrupción.

Fuente: Realizado por Ximena Domínguez Campuzano con base en los cables diplomáticos analizados.

4.3 ¿Violación de Soberanía Nacional?

Con las revelaciones de los diplomáticos norteamericanos ubicados en diversos países surgió el cuestionamiento de si las políticas de espionaje instrumentadas por el gobierno de los Estados Unidos podrían ser consideradas como una violación a la soberanía nacional, al intervenir comunicaciones privadas en países externos. Sin embargo, el problema se volvió más complejo frente a la discusión

de si los que realizaron las intervenciones telefónicas fueron empresas nacionales o norteamericanas.

Un caso que ejemplifica este proceso es la revelación de las escuchas telefónicas por parte la NSA de la presidenta Dilma Rousseff. Ella argumentó que si hubo violación **"**Si hubo participación de otros países o de otras empresas no brasileñas"[273]. Es decir, desde su perspectiva es una violación a la soberanía nacional, si el espionaje es realizado por empresas extrajeras. Adicionalmente, argumenta que el problema significa una violación a los derechos humanos de las personas involucradas, ya que no pidieron autorización para dar a conocer su información personal.

El principal problema para entender si las prácticas de espionaje constituyen una violación a la soberanía nacional de los Estados radica en el hecho de que hasta el momento no existe ningún instrumento de derecho internacional que regule esta actividad. Sin embargo se ha sostenido que bajo el principio de no intervención en asuntos de jurisdicción interna de los Estados, se podría considerar a las actividades de espionaje como una violación a la soberanía nacional amparándose en la Resolución 2625 de la Asamblea General de la Organización de Nacionales Unidas en donde se establece que:

> "*Ningún Estado o grupo de Estados tiene derecho a intervenir directa o indirectamente, y sea cual fuere el motivo, en los asuntos internos o externos de cualquier otro. Por tanto, no solamente la intervención armada, sino también cualesquiera otras formas de injerencia o de amenaza atentatoria de la personalidad*

[273]DPA, *Rousseff asegura que Brasil investigará "violación de soberanía" en caso de espionaje de EEUU*, [en línea], La tercera, 8 de julio de 2013, Dirección URL: http://www.latercera.com/noticia/mundo/2013/07/678-532079-9-rousseff-asegura-que-brasil-investigara-violacion-de-soberania-en-caso-de.shtml, [Consultado el 18 abril de 2014].

del Estado, o de los elementos políticos, económicos y culturales que lo constituyen, son violaciones del Derecho Internacional"[274].

Por lo que cualquier actividad de vigilancia y espionajes sin previa autorización del Estado podría ser considerada como una violación a la soberanía nacional.

Por otra parte, el caso de Wikileaks también ha generado polémica respecto a si la difusión de la información de esta organización ante los medios de comunicación y dentro de Internet está afectando o violando la soberanía de los Estados Unidos o alguna norma estadounidense.

La opinión pública en términos generales ha señalado "los documentos de Wikileaks no parecen violar el derecho norteamericano, ni por la ley de espionaje ni por la de comunicaciones. La obligación de proteger la confidencialidad de los secretos de Estado corresponde a los gobierno, no a los medios de comunicación ni a los particulares"[275].

También David Carr ha evidenciado en un artículo del New York Times que esta organización como tal no podría ser castigada si se encontrara que está violando alguna ley, porque "Wikileaks se erige en el máximo exponente de la desterritorialización. Estamos ante un <mecanismo trasnacional para difundir información fuera del alcance de cualquier gobierno, empresa u organización>"[276]. Sin embargo, reconoce que existen sustentos jurídicos para establecer un juicio

---

[274] Resolución 2625 (XXV) de la Asamblea General de Naciones Unidas, Declaración relativa a los Principios de Derecho Internacional referentes a las relaciones de amistad y a la cooperación entre los Estados de conformidad con la Carta de las Naciones Unidas, [en línea], Dipublico.com.arg, 24 de octubre de 1970, Dirección URL: http://www.dipublico.com.ar/3971/resolucion-2625-xxv-de-la-asamblea-general-de-naciones-unidas-de-24-de-octubre-de-1970-que-contiene-la-declaracion-relativa-a-los-principios-de-derecho-internacional-referentes-a-las-relaciones-de/, [Consultado el 5 de mayo de 2014].

[275] Damián Loreti y Luis Lozano, *El caso Wikileaks y su relación con el derecho a la información*, [en línea], Catedra, p 9. Dirección URL:http://www.catedras.fsoc.uba.ar/loreti/documentos_de_la_catedra/wikileaksdali.pdf, [Consultado el 5 de mayo de 2014].

[276] Alberto Pampin Quian, *El impacto mediático y política de WikiLeaks*. La historia más apasiónate del periodismo moderno, Editorial UOC, España, 2013.

en contra del creador de esta organización, es decir, Julian Assange, como está sucediendo.

4.4 ¿Violación de derechos Humanos?

El caso de Wikileaks ha conllevado varios cuestionamientos: uno de ellos gira en torno a si esta constante vigilancia por parte de las agencias de inteligencia, y en general del gobierno estadounidense puede ser considera como una violación a los derechos humanos. Se ha argumentado que la privacidad es un derecho fundamental de todos los ciudadanos, establecido en la Declaración Universal de los Derechos Humanos en el artículo 12: "Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia"[277], por lo cual consideran que las políticas de vigilancia están violando este derecho fundamental al intervenir conversaciones.

De igual manera el artículo 19 de esta Declaración Universal de los Derechos Humanos plantea que:

> *"Todo individuo tiene derecho a la libertad de opinión y de expresión; este derecho incluye el de no ser molestado a causa de sus opiniones, el de investigar y recibir informaciones y opiniones, y el de difundirlas, sin limitación de fronteras, por cualquier medio de expresión".*[278]

Además de estos postulados de la Declaración Universal de Derechos Humanos, debemos tener en cuenta que existe una instancia internacional denominada "Principios de Johannesburgo sobre Seguridad Nacional, Libertad de Expresión y

---

[277]Véase: Declaración Universal de los Derechos Humanos, [en línea], CINU, Dirección URL:http://www.cinu.mx/onu/documentos/declaracion-universal-de-los-d/, [Consultado el 7 de mayo de 2014].

[278]Véase: Declaración Universal de los Derechos Humanos, CINU, Dirección URL:http://www.cinu.mx/onu/documentos/declaracion-universal-de-los-d/, [Consultado el 1 de mayo de 2014].

acceso a la información"[279] creada en 1995 que ayudan a determinar hasta qué punto los gobiernos pueden ocultar información al público. De estos principios para el caso de Wikileaks podemos aplicar varios artículos (Ver Anexo 1), donde se demuestra que el acceso a la información y la trasparencia tiene algunos límites dentro de los que se encuentra la seguridad nacional, siempre y cuando existe una justificación demostrable y la adecuada aplicación de leyes.

Sin embargo, en el caso de la información dada a conocer por Wikileaks no se cumple estos principios de libertad de expresión y acceso a la información, ya que es información clasificada, pero en su mayoría no es información que afecte la seguridad nacional, por lo que no se puede justificar que no sea de libre acceso.

Por otra parte, los relatores especiales de las Naciones Unidad para la Protección y Promoción del Derecho a la Libertad de Opinión y de Expresión, así como la Relatora Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos han abordado también el tema planteando en 2010 señalando lo siguiente: "El derecho de acceso a la información en poder de autoridades públicas es un derecho humano fundamental sometido a un estricto régimen de excepciones"[280]. Lo cual nos demuestra que para las instancias internacionales la trasparencia y acceso a la información por parte de los gobiernos se ha convertido en un derecho humano basado en el principio de generar gobiernos más funcionales y democráticos.

---

[279] Estos principios fueron establecidos por el Centro Internacional Contra la Censura en colaboración con el Centro de Estudios Legales Aplicados de la Universidad de Witwatesrand. Fueron aprobados por el Relator Especial para la Libertad de Opinión y Expresión de la ONU Abid Hussain. Véase: Los Principios de Johannesburgo sobre la Seguridad Nacional, la Libertad de Expresión y el Acceso a la Información, Articulo 19, [en línea], Noviembre 1996, Dirección URL:http://www.corteidh.or.cr/tablas/a22440.pdf, [Consultado el 8 de mayo de 2014].

[280] Relatores especiales de la OEA y ONU, *Declaración Conjunta sobre Wikileaks*, [en línea],OEA, 21 de diciembre 2010, Dirección URL:http://www.oas.org/es/cidh/expresion/showarticle.asp?artID=829&IID=2, [Consultado el 2 de mayo de 2014].

Todo ello nos lleva a reflexionar que si bien es cierto que el gobierno norteamericano justifica sus actividades de espionaje y vigilancia bajo el principio de protección de su seguridad nacional, no toma en cuenta las prioridades de seguridad de los otros Estados. Tampoco acepta el espionaje de otros estado en su territorio, aunque él si lo aplica y ejerce.

Asimismo, el argumento de la seguridad interna cae en contradicción con la importancia de respetar los derechos humanos de los otros, al no tomar en cuenta el derecho a evitar que la información personal sea difundida sin autorización de la persona involucrada

Finalmente, es necesario tomar en cuenta que el gobierno norteamericano ha argumentado que él no cometió la violación, sino Wikileaks, quien dio a conocer la información clasificada sobre individuos, instituciones, gobiernos sin su consentimiento. Argumentó que bajo el principio de generar gobiernos más trasparentes, también están incurriendo en una violación a la privacidad y a la libertad de expresión de los actores involucrados. Sin embargo, evade su responsabilidad sobre la información recuperada. Ello ha llevado a plantear la necesidad de establecer un equilibrio entre seguridad nacional y privacidad para lograr de esta manera una sociedad libre[281]

[281] Cita textual en ingles: "The need to strike a balance between security and privacy is a constant challenge, and it's the mark of a free society that we debate that balance vigorously and in public". Schiff Adam B., An NSA fix, Los Angeles Times, 31 de octubre 2013, Dirección URL:http://www.latimes.com/opinion/commentary/la-oe-schiff-nsa-surveillance-phone-metadata--20131031,0,4107687.story#axzz2v3AJyByI, [Consultado el 8 de mayo de 2014].

Conclusiones

De esta investigación podemos concluir en primer lugar que en la actualidad las Relaciones Internacionales implican ya no solamente una relación entre Estados, sino que el proceso de globalización derivado del desarrollo descomunal de las comunicaciones ha configurado una mutación de la dinámica mundial, particularmente en el ciberespacio, donde se requieren acuerdos internacionales con la finalidad de que este, con sus múltiples dimensiones, permita la protección de intereses, derechos y libertades. Sin embargo, es necesario tomar en cuenta que el nuevo fenómeno ya no es exclusivamente una preocupación de los Estados, sino también de las empresas y corporaciones, así como de los individuos de todo el mundo, de ahí la importancia de haber analizado este tema.

El ciberespacio requiere de respuestas a una multitud de intereses en juego, derivados de sistemas políticos, económicos y jurídicos diferentes, pero también con desarrollos tecnológicos diferentes, cuyo tratamiento requiere de cierta armonización para lograr equilibrios entre los intereses en juego, ya que de lo contrario los desequilibrios hoy presentes serán una constante.

Las redes digitales han sido un instrumento de desarrollo, pero ahora también implican nuevos desafíos en materia de seguridad. La nueva dinámica ha mostrado que el Ciberespacio y las relaciones electrónicas que lo sustentan son un nuevo valor internacional que debe ser protegido jurídicamente. Sin embargo, el enorme problema estriba en cómo lograr estos acuerdos, porque dichos lineamientos entran en contradicción con algunas de las estrategias en materia de seguridad nacional del gobierno norteamericano.

En general, como lo enuncia la hipótesis de esta tesis, fue a partir de los atentados terroristas del 11 de septiembre que el gobierno de los Estados Unidos asumió como su principal prioridad resguardar la Seguridad Nacional, y por ende incrementó las políticas para asegurar el ciberespacio y proteger la infraestructura crítica de futuras amenazas.

Razón por la cual durante las administraciones de los presidentes George W. Bush y Barack Obama se crearon Estrategias de Seguridad Nacional Cibernéticas y el tema se incorporó como una de sus prioridades nacionales. Se establecieron diversas medidas para disminuir las vulnerabilidades en el ciberespacio y generar una concientización sobre la importancia de establecer políticas en esta materia. Como parte de esta estrategia se crearon una serie de leyes y reglamentos para fortalecer la seguridad de Estados Unidos en el ciberespacio y las agencias de inteligencia ampliaron sus medidas de vigilancia ante posibles amenazas extranjeras.

La política de seguridad interna se materializó durante el gobierno de George Bush en un endurecimiento de las políticas de vigilancia por parte de las agencias de inteligencia, así como en el incremento de sus atribuciones, lo cual permitió que el gobierno no sólo realizara labores de espionaje en el exterior, sino también en el interior del país. Adicionalmente, implementó medidas de vinculación entre el sector público y privado como estrategia para ampliar la recolección de información. Sin embargo, dicha medida, que originalmente había sido planteada como una necesidad en materia de seguridad, se convirtió en el mediano plazo en una debilidad, al disminuir los controles sobre la información, lo cual abriría la puerta para la fuga de información. Sin embargo, dicho efecto se observaría hasta la gestión de Obama.

Por otra parte, la administración de Barack Obama tuvo una posición más activa en las políticas cibernéticas. Destacó los peligros y amenazas que significaba para el país un posible ataque cibernético, por lo que centró sus esfuerzos en eliminar las debilidades de los sistemas cibernéticos gubernamentales en dos niveles. Por una parte, continuó fortaleciendo las alianzas estratégicas entre el sector privado y el gubernamental y por la otra amplió las políticas de capacitación y concientización, como medidas para asegurar el ciberespacio. Se definieron a las políticas de seguridad cibernética como una prioridad de seguridad nacional, al afirmar que un ataque contra los sistemas digitales gubernamentales afectaría a

todo el país y podría tener consecuencias económicas y políticas, por ello era considerado un tema de vital interés de todos los norteamericanos. Es decir, las autoridades destacaron que la seguridad del ciberespacio no era sólo un problema que afectaba al gobierno, sino que también podía tener efectos devastadores para el sector privado o la ciudadanía, de ahí la importancia de esta alianza.

Bajo la premisa de que el ciberespacio, es un área de confluencia de intereses de la más variada índole (públicos y privados, estatales, comerciales, industriales, individuales, sociales, militares, de inteligencia o policiales), el gobierno de Obama buscó establecer lazos de coordinación y cooperación a nivel internacional para asegurar las redes de comunicación y enfrentar las nuevas amenazas cibernéticas el momento.

Sin embargo a pesar de estas medidas y leyes instrumentadas durante estas administraciones, el caso Wikileaks mostró que la subcontratación de empresas privadas y tanto de personal de inteligencia como de tecnología, se ha convertido en un problema para la Comunidad de Inteligencia de los Estados Unidos. En primer lugar porque abre la posibilidad de que un gran número de personal tenga acceso a información clasificada, lo que dificulta su supervisión y hace más fácil que algún miembro de esta cadena de personal filtre alguna información sin ser detectado rápidamente. Aunado, al gran número de información que se encontraba dentro de los sistemas cibernéticos, lo que dificultó su resguardo y vigilancia, haciendo más fácil una filtración.

En segundo lugar, porque el incremento de la subcontratación como una medida para asegurar los sistemas gubernamentales con la tecnología más avanzada, ha representado altos costos para el presupuesto de inteligencia del gobierno, alcanzando montos superiores a los programas militares y la mayor parte de estos recursos se destinan a pagar empresas privadas, demostrando que la subcontratación de empresas privadas ha resultado más costoso para el gobierno

federal, que capacitar al personal interno para realizar estas tareas. Asimismo esta subcontración demuestra que las agencias de inteligencia no contaban con el personal capacitado para manejar algunos programas cibernéticos, ni con las innovaciones tecnologías, para realizar sus actividades de inteligencia de manera autónoma.

En tercer lugar porque estas empresas privadas, no están rindiendo cuentas de sus acciones ante ninguna instancia gubernamental, a pesar de que están jugando un papel más importante en las actividades de inteligencia. Lo cual es preocupante porque significa que el gobierno federal está delegando sus principales responsabilidades.

A lo largo de esta tesis, mostramos que la NSA y la CIA son las agencias que más reciben presupuesto. Teniendo la primera mayores atribuciones en el ciberespacio, mientras que la segunda ha operado de manera preponderante a partir de intervenciones diplomáticas.

La filtración de información también hizo evidente primero que las políticas de espionaje y vigilancia implementadas por el gobierno norteamericano no fueron eficientes al permitir el acceso a información reservada sin ser detectados y segundo que las agencias de inteligencia abusaron de estas políticas de espionaje y no rindieron cuentas de sus actividades ante ninguna instancia de representación gubernamental (Congreso o el Presidente de los Estados Unidos).

Se puede concluir que el control por parte del Congreso sobre las actividades de inteligencia ha sido deficiente, porque los Comités de Inteligencia no realizan una verdadera supervisión de estas actividades y han evadido su responsabilidad sobre las actividades de espionaje. El Congreso ha argumentado en todo momento conflictos jurisdiccionales, lo cual parece tener fundamento. Sin embargo, no han realizado ninguna acción para combatir los problemas

existentes, sólo de manera aislada algunos legisladores externaron críticas, pero no se ha observado una preocupación institucional por el tema.

Se pudo evidenciar en la tesis, que el hecho de que los Comités de Inteligencia no estén supervisando estas actividades, significa que en la práctica política no existe la posibilidad de generar pesos y contrapesos, base del equilibrio del sistema presidencial norteamericano. Ello ha provocado conflictos entre el Congreso y el Ejecutivo, ya que ambos quieren deslindarse de cualquier tipo de responsabilidad, argumentando que no estaba dentro de su ámbito de competencia.

Esta situación se ha traducido en vacíos jurídicos que han permitido a las agencias de inteligencia tomar decisiones sin autorización o supervisión de las instancias gubernamentales encargadas, lo cual es preocupante, ya que no queda claro quién está al mando de estas actividades de espionaje, cuáles son sus objetivos y razones por las que se están realizando y cuál es el manejo que se le da a la información obtenida.

También a lo largo de esta investigación constatamos la existencia de problemas estructurales que impiden al Congreso realizar una verdadera supervisión de las agencias de inteligencia. Agencias como la NSA, desde su creación, no tienen la obligación de rendir cuentas ante el Congreso de las actividades que realizan, lo que les da la posibilidad de realizar escuchas telefónicas y espiar correos electrónicos de manera indiscriminada y sin ningún tipo de supervisión, lo cual atenta contra la seguridad de los usuarios de Internet y la información reservada de los ciudadanos.

La participación de accionistas o directores de empresas privadas de ex miembros de la comunidad de inteligencia, ha llevado también a pensar que existen grupos interesados en continuar con estas subcontratación ya que representan grandes ganancias para ellos. Esto podría explicar por qué no han

hecho nada para disminuirlas, a pesar de los importantes costos y problemas que están generando en las actividades de inteligencia.

Por tal razón parece de vital importancia que se limite la subcontratación de empresas privadas y se canalicen estos recursos a la innovación, la capacitación y la educación. También parece relevante que el gobierno federal retome el control de las agencias de inteligencia, manteniendo una verdadera supervisión de sus actividades y se realice una exhaustiva evaluación de todas las políticas cibernéticas y de inteligencia como medida para evitar futuras filtraciones de información.

Por otra parte, debemos hacer hincapié en el hecho de que tras la filtración de datos clasificados de Wikileaks se esperaban cambios en distintos niveles que modificaran las cosas dentro del gobierno. No obstante, en la práctica, solamente hubo un incremento de las medidas de seguridad, de restricción del flujo de los datos y una mayor vigilancia del personal a cargo de esta información. Es decir, hubo cambios en los aspectos técnicos de los protocolos de seguridad, pero no en el fondo de esta dinámica.

Asimismo, estas revelaciones evidenciaron que las actividades de vigilancia y espionaje no solamente se aplican a sospechosos de delitos o posibles amenazas al gobierno de los Estados Unidos, sino que se han convertido en una constante y se vigila tanto a extranjeros como nacionales. Lo que generó fuertes cuestionamientos en la opinión pública sobre los motivos de la constante vigilancia, así como sobre la violación a los derechos humanos y a la soberanía de los Estados que esta política implica.

A nivel externo, la revelación de los cables diplomáticos operó como prueba de que el gobierno de los Estados Unidos mantenía una política de espionaje y recolección de información por parte de sus diplomáticos en todo el mundo, no sólo de las posturas ideológicas y políticas, sino también de la información

reservada de los funcionarios de otros países. Este hecho no se justificaba después de terminada la guerra fría y demostró las contradicciones de la diplomacia estadounidense sobre lo que se dice de manera pública y lo que en realidad se hace. También rompió con el paradigma de integridad y trasparencia manejada por el gobierno de Estados Unidos, al mostrar una realidad diferente.

Este caso evidenció la doble función de los diplomáticos estadounidenses, que fungen como representantes de política exterior y también como espías, lo cual mostró que las actividades de inteligencia son prioritarias para los Estados Unidos. Al mantener una constante vigilancia de los presidentes y primeros ministros de diferentes gobiernos en su vida privada, horarios de trabajo, personalidad, estado de salud y respuesta ante situaciones complicadas, el gobierno estadounidense incumple los acuerdos en materia de información reservada y confidencial, pero también el respeto a la soberanía de los estados.

La filtración de los *Cablegates* solo generó fricciones diplomáticas en algunos países como México y Ecuador, donde se registró la expulsión de los embajadores norteamericanos en funciones, como forma de cuestionamiento a las políticas de espionaje emprendidas por el gobierno de los Estados Unidos.

A pesar de que algunos de los comentarios y datos revelados por estos cables pudieron haber causado mayor conmoción y cuestionamiento, los Jefes de Estado afectados como Italia, China y Alemania simplemente externaron su malestar ante la opinión pública, sin realizar ningún cambio institucional en sus relaciones con el gobierno estadounidense, al considerar que estas revelaciones no eran motivo de un conflicto diplomático. Es decir, las consecuencias de estos cables fueron básicamente mediáticas.

Algunos miembros del gobierno se manifestaron indignados y solicitaron explicaciones no al gobierno estadounidense sino a sus propios gobiernos por las acciones, evasiones, corrupciones y malas prácticas que estaban realizando. Es decir, las filtraciones de información más que debilitar al gobierno norteamericano

afectaron a los gobiernos de los cuales se dio a conocer información, porque operó como elemento de prueba de las irregularidades prevalecientes.

Una de las repercusiones más graves en material de diplomacia de Wikileaks es que a partir de ese momento tanto sus homólogos como los altos funcionarios tendrán más cuidado sobre los la información y los comentarios que realizan ante los diplomáticos estadounidenses, lo cual significará la pérdida de detalles e información relevante sobre lo que está ocurriendo en otros países para el gobierno de los Estados Unidos. La posible falta de confianza hacia los diplomáticos norteamericanos podría convertirse en un grave problema para la política exterior norteamericana, ya que podría disminuir el suministro de información que es una base fundamental para las negociaciones y alianzas que emprende este gobierno con el resto del mundo.

Con respecto al derecho internacional, las revelaciones de Wikileaks evidenciaron la necesidad de establecer a través de un tratado o un acuerdo internacional lineamientos claros en materia de espionaje. Porque hasta el momento no existe un tratado sobre la materia, lo cual genera un vacío jurídico y falta de regulación hacia estas prácticas.

También es preciso hacer un cuestionamiento sobre la política de Seguridad Nacional de los Estados Unidos, que ha llevado a rebasar los límites territoriales de su Estado, promoviendo políticas de espionaje más allá de sus fronteras. El espionaje no solamente es utilizado por el gobierno estadounidense para enfrentar amenazas externas que puedan desestabilizar al país, sino que se han convertido en un mecanismo para conseguir información y ventajas comparativas durante las negociaciones y alianzas internacionales. Esta dinámica pone a discusión hasta donde llegan los límites para lograr la seguridad estatal y si es preciso violar derechos individuales en razón de la seguridad nacional o si esta actuación representa una violación al derecho de privacidad por parte del Estado. Adicionalmente, pone a discusión la falta de respeto a la soberanía estatal, al

derecho a la privacidad, así como a los derechos humanos de los ciudadanos del mundo.

También Wikileaks puso en la mesa de debate el papel de los medios de comunicación ante el acceso a información clasificada, sobre si es válido presentar información secreta obtenida por el gobierno ante la ciudadanía, basándose en el principio de trasparencia y libertad de prensa o si esto constituye una manipulación de la información al exponerse sin un análisis previo y una contextualización la información clasificada. Las revelaciones de Wikileaks llevaron a cuestionar si los medios de comunicación bajo el principio de libertad de expresión tienen el derecho a publicar cualquier información de la que dispongan sin valorar las consecuencias jurídicas, políticas y diplomáticas que puede traer consigo la revelación de los datos.

Es importante destacar que las prácticas de espionaje por parte de los embajadores no han desaparecido, sólo cambió la forma en que se realizan estas comunicaciones. Es probable que hayan disminuido las intervenciones de las agencias en comunicaciones privadas por la presión de la opinión pública. Sin embargo, parece difícil que esta dinámica se abandone, porque son los principales medios de recopilación de información que tiene el gobierno de los Estados Unidos, los cuales se justifican para el mantenimiento de su Seguridad Nacional.

Dentro del gobierno de los Estados Unidos existe una constante contradicción entre el principio de democracia y el secretismo. Por una parte se define como un país democrático y representativo que exige trasparencia y rendición de cuentas de todos los gobiernos ante la ciudadanía. Sin embargo, por otra parte, a nivel internacional, su prioridad es asegurar su seguridad nacional, utilizando a las agencias de inteligencia como medio para obtener de información secreta que permita anticiparse a las amenazas, pero también utilizarla de manera estratégica en las relaciones internacionales, aprovechando las ventajas que le da contar con

información privilegiada, sin tomar en cuenta la violación a las fronteras estatales y los derechos internacionales.

Como conclusión final podemos decir que el caso de los *Cablegates* de Wikileaks fue trascendental porque: 1) permitió saber que las agencias de inteligencia de los Estados Unidos recopilan información de todo el mundo a través de los diplomáticos y que violan la información reservada de funcionarios de otros Estados, lo cual contradice los Tratados Internacionales en la materia y generó la condena de la comunidad internacional mediante el espionaje electrónico; 2) se constató que los diplomáticos estadounidenses enfocan sus actividades en mantener informado a su país de origen sobre la situación y los temas de mayor trascendencia para sus intereses particulares, más que en el establecimiento de negociaciones detrás de escena; 3) que existen documentos que pueden contribuir a explicar cuál fue la lógica del Departamento de la Defensa en determinados conflictos y cuáles fueron las estratégicas que implementó en diversas situaciones; 4) muestran los nexos de empresas de inteligencia privada con organismos de inteligencia de Estados Unidos y la oposición a difundir información reservada en la red, lo cual confirma que el gobierno de Barack Obama, lejos de alejarse del secretismo de la era Bush se opone fuertemente a la transparencia; 6) proyecta la imagen de un Estado que no ha respetado el ejercicio democrático, que no ha respetado los derechos humanos y que tiene como prioridad sus intereses estratégicos en materia de seguridad nacional; 7) muestra que la política de seguridad cibernética es una prioridad nacional del gobierno norteamericano.

Bibliografía

- Assange Julian; Appelbaum Jacob; *et. al*, *Cypherpunks: La Libertad y el futuro del Internet*, España, Ed. Grupo Planeta, 2013, 224 páginas.
- Aguayo Quezada Sergio y Bagley Bruce Michael, *En busca de la Seguridad Pérdida. Aproximaciones a la seguridad nacional mexicana*, México, Ed. Siglo XXI, 2002, 417 páginas.
- Banks William C., *National Security Law and the Power of the Purse*, Estados Unidos, Ed. Oxford University Press, 1994, 272 páginas.
- Bartlett Manuel, *El país a debate: Una crítica urgente contra el gobierno conservador y antinacional*, México, Ed. Grijalbos, 2012, 343 páginas.
- Baylis John, Wirtz James Gray Colin S. y Cohen Eliot, *Strategy in the contemporary world*, Estados Unidos, Ed. Oxford University Press, 2007, 392 páginas.
- Beckett Charlie; Ball James, *Wikileaks News in the Network Era*, Gran Bretaña, Ed. Polity Press, 2012 198 páginas.
- Bengareche Borja, *Wikileaks confidencial*, España, Ed. Anaya Mutimedia, 2011, 213 páginas.
- Calduch Rafael, *Relaciones Internacionales*, Madrid, Ed. Ediciones Ciencias Sociales, 1991, 450 páginas.
- Chadwich Andrew, *Internet Politics,* Estados Unidos, Ed. Oxford Press, 2006, 384 páginas.
- Cooper Andrew F.; Ieine Jorge; Thakur Ramesh, *The Oxford Handbook of Modern Diplomacy*, Reino Unido, Ed. Oxford University Press, 2013, 953 páginas.
- Cotino Hueso Lorenzo (Coord), *Libertades, democracia y gobierno electrónicos,* España, Ed. Comares, 2006, 339 páginas.
- Czosseck Christian y Geers Kenneth, *The Virtual Battlefield: perspectives on Cyber Warfare*, Amsterdam, Ed. IOS Press, 2009, 307 páginas.

- Davison Neil, *Non-Leathal Weapons*, Estados Unidos Ed. Palgrave Mcmillan, 2009, 304 páginas.
- Debra Miller A. Politic and the Media, Estados Unidos, Ed. Greenhaven Press, 2012, 192 páginas.
- Dening Doroty E., *Information Warface and Security,* Ed. Addison Wesley Longman, Estados Unidos, Enero 2000, 522 páginas.
- Escribano Úbeda-Portugués José, *Lecciones de Relaciones Internacionales*, Madrid, Ed. Aebius, 2010, 362 páginas.
- Esteban Navarro Miguel Ángel, (Coord), *Glosario de Inteligencia*, España, Ministerio de Defensa de España, 2007 118 páginas.
- Estulin Daniel, *Deconstructing Wikileaks*, Estados Unidos, Ed. Independent Publishers Group, 2012, 189 páginas.
- Fuentes Claudio, *Bajo la mirada del halcón: Estados Unidos-América Latina post 11/9/2001*, Chile, Ed. Biblos, FLACSO, 2004, 260 páginas.
- Griffiths Spielman John, *Teoría de la seguridad y defensa en el continente americano*, Chile, Ed. RIL editores, 2011, 642 páginas.
- Gutiérrez Rubí Antoni, *La política vigilada: La comunicación política en la era de Wikileaks*, España, Ed. UOC, 2011, 157 páginas.
- Herrera Hermosilla Juan Carlos, *Breve Historia del Espionaje,* España, Ediciones Nowtilus, 2012, 304 páginas.
- International Business Publications, Inc, *US Central Intelligence Agency (CIA) Handbook-Strategic Information*, [en línea], Estados Unidos, Ed. International Business Publications, Inc, 2013, Pp. 18-19, Dirección URL: http://books.google.com.mx/books?id=4VubAAAAQBAJ&pg=PA18&lpg=PA18&dq=%E2%80%9Cthe+U.S.+intelligence+budget+in+fiscal+year+2012+was+$53.9+billion,&source=bl&ots=-I8TVWdsts&sig=v0On3Ai_tPi4HwLOXzZgazzO-2I&hl=es&sa=X&ei=XVZyU_uZN-TL8QH5jIGYDw&ved=0CIoBEOgBMAg#v=onepage&q=%E2%80%9Cthe%20U.S.%20intelligence%20budget%20in%20fiscal%20year%202012%20was%20%2453.9%20billion%2C&f=false,
- Janczewski Lech J.; Colarik Andrew M., *Cyber Warfare and Cyber Terrorism,* Estados Unidos, Ed. Information Science Reference, 2008, 532 páginas.

- Kramer Franklin D.; Starr Stuart H.; Wentz Larry K., *Cyberpower and National Security*, Estados Unidos, Ed. Center for Technology and National Security Policy, 2009, pp. 26-27.
- Losh Elizabeth, *Virtualpolitik,* Estados Unidos, Ed. Masachusetts Institute of Technology, 2009, 414 páginas.
- McAvoy Nelson, *Coded Messages: How the CIA and NSA Hoodwink Congress and the People*, Estados Unidos, Ed. Algora Publishing, 2010, 212 páginas.
- Merle Marcel, *Sociología de las relaciones internacionales*, Madrid, Ed. Alianza Universitaria, 1978, 461 páginas.
- Oswald Spring Úrsula y Gunter Brauch Hans, *Reconceptualizar la seguridad en el siglo XXI,* México, Ed. UNAM, 2009, 887 páginas. Dirección URL:http://www.crim.unam.mx/drupal/?q=node/407
- Pampin Quian Alberto, *El impacto mediático y política de WikiLeaks. La historia más apasiónate del periodismo moderno,* España, Editorial UOC, 2013, 124 páginas.
- Pérez Jorge y Badía Enrique, *El debate sobre la privacidad y seguridad en la Red: Regulación y mercados,* España, Ed. Ariel y Fundación Telefónica, diciembre 2012, 202 páginas.
- Rivera Vélez Fredy, Inteligencia estratégica y Prospectiva, FLACSO, Ecuador, Mayo 2011, 296 páginas.
- Romero Alberto, *Globalización y pobreza*, Colombia, Ed. Universidad de Nariño, marzo 2002, 161 páginas.
- Sagal Rahul, *Secrets and leaks: the dilemma of state secrecy*, Estados Unidos, Ed. Princeton University Press, 2013, 304 páginas.
- Salazar Ana María, *Seguridad Nacional Hoy. El reto de las democracias*, México, Ed. Nuevo Siglo Aguilar, 2002, 375 páginas.
- Sampedro Blanco Víctor, *Opinión pública y democracia deliberativa*, España, Ediciones Istmo, 2000, 217 páginas.
- Shorrock Tim, *Spies for Hire: The Secret World of Intelligence Outsourcing*, Estados Unidos, Ed. Simon & Schuster, 2008, 464 páginas.

- Star Alexander, *Open Secrets: Wikileaks, War and American Diplomacy*, Estados Unidos, Ed. The New York Times, 2011, 608 páginas.
- Sodupe Kepa, *La teoría de las Relaciones Internacionales a comienzos del Siglo XXI,* Bilbao, Ed. Universidad del País Vasco, 2003, 254 páginas.
- Toffler Alvin y Heidi, *Las guerras del futuro*, España, Ed. Plaza & Janes Editores, 1995, 416 páginas.
- Thompson Tamara, Wikileaks, Estados Unidos, Ed. Greenhaven Press, 2012, 120 páginas.
- Valdés Ugalde José Luis; Valdés Diego, *Globalidad y conflicto Estados Unidos y la crisis de septiembre,* México, Ed. UNAM/CISAN, agosto 2005, 369 páginas.
- Whitaker Red, *El fin de la privacidad. Cómo la vigilancia total se está convirtiendo en realidad*, España, Ed. Paidós, 1999, 238 páginas.

Hemerografía

- Aguirre Mariano, "La estrategia de seguridad en la nueva época Bush: la guerra preventiva y la ideología del imperio", *Revista Internacional de Filosofía Política*, México, Ed. UAM Iztapalapa, Julio 2003, No. 21, Pp. 236-242.
- Barbé, Esther, "El papel del realismo en las relaciones internacionales. La teoría de la política internacional de Hans J. Morgenthau", *Revista de Estudios Políticos*, España, 1987, Núm. 57, pp. 149-176.
- Bush George W., "La estrategia de seguridad nacional de los Estados Unidos de América", *Revista Internacional de Filosofía Política*, México, Ed. UAM Iztapalapa, Julio 2003, No. 21, Pp. 201-235.
- González Paras José Natividad, "Los servicios de inteligencia en el nuevo siglo", *Revista de Administración Pública*, México, Núm. 101, INAP, 2000. pp. 143-165.
- Johan Eriksson; Giampiero Giacomello, "Information Revolution, Security, and International Relations; (IR) relevant Theory?", *International Political Science Review*, Núm. 3, Vol. 27, Estados Unidos, Ed. Sage Publications, 2006, pp. 221-244.

- Mabel Laredo Iris, “Incidencia de los grupos de presión en la formulación y control de la política internacional”, *Revista de El Colegio de México, Foro Internacional*, México, Núm. 1, Vol. 6, Julio-Septiembre 1965, Pp. 136-194.
- Mendes Cardoso Alberto, *El papel de la actividad de inteligencia* en el inicio de una nueva era, en “Los servicios de inteligencia en el nuevo siglo”, *Revista de Administración Pública*, Núm. 101, México, INAP, 2000, Pp. 20-30.
- Miranda V. Carlos, “Realismo e idealismo en el Estadio de las Relaciones Internacionales: la influencia de Hobbes y de Kant”, *Revista de Ciencia Política*, Núm. 95, Vol. VIII, Chile, 1986, Pp. 88- 100.
- Miranda V. Carlos, “Hobbes y la anarquía internacional”, *Revista de Ciencias Políticas*, Chile, Núm. 2, Vol. VI, 1984, Pp. 71 a la 84.
- Orozco Restrepo Gabriel Antonio, “El aporte de la Escuela de Copenhague a los estudios de seguridad”, *Revista Fuerzas Armadas y Sociedad*, Chile, FLACSO, Núm. 1, Año 20, Pp. 141-162.
- Salomón González Mónica, “La Teoría de las Relaciones Internacionales en los albores del siglo XXI, dialogo, disidea, aproximaciones”, *Revista CIDOB d’Afers Internacionales***,** España, Num.56, 2003, 52 páginas.
- Soltero Gonzalo, “WikiLeaks: los cables sobre México”, *Revista Casa del Tiempo*, México, Ed. UAM, Núm. 45-46, Vol IV, Época IV, Julio-agosto 2011, Pp.44-48.
- William J, Lyns, “Defending a New Domain - The Pentagon's Cyberstrategy”, Estados Unidos, *Revista Foreign Affairs,* Núm. 5, Vol. 89, septiembre/octubre de 2010, Pp. 97-108
- s/a, “Inteligencia y seguridad”, *Revista de análisis y prospectiva*, Madrid, Ed. Universidad Rey Juan Carlos y Universidad Carlos III de Madrid, Núm. 4 Julio-noviembre 2008, 241 páginas.

Tesis

- Camberos Yáñez Yahel Fabiola, *La seguridad en Norteamérica dentro del marco del comando Norte: la experiencia de México y Canadá (1994-2010),* México, UNAM, Facultad de Estudios Superiores Aragón, 2011, 242

páginas. (Licenciado en Relaciones Internacionales, asesor David García Contreras)

- Cruz Lugargo Pedro Isnardo, *La seguridad nacional en Estados Unidos de América: Toma de decisiones presidenciales en escenarios de crisis: George W. Bush (2001-2008),* México, UNAM, Facultad de Ciencias Políticas y Sociales, 2011, 469 páginas. (Doctor en Ciencias Políticas y Sociales)
- Bustamante Castellanos Araceli del Carmen, La Agencia Central de Inteligencia de Estados Unidos en el marco del Derecho Internacional y la política mundial, UNAM, Facultad de Ciencias Políticas y Sociales, 2009, 162 páginas. (Licenciatura en Relaciones Internacionales, Asesor Velázquez Elizarrarás Juan Carlos)
- González Reyes, Andrei Antonio, Estados Unidos de América y la Agencia Central de Inteligencia como elementos desestabilizadores del Medio Oriente: (caso Irán), UNAM, Facultad de Ciencias Políticas y Sociales, Diciembre 2012,163 páginas. (Licenciatura en Ciencias Políticas y Administración Pública, Asesor Muñoz Víctor Manuel)
- Méndez de la Brena Dresda Emma, *Biopoder como elemento de Seguridad Nacional,* México, Universidad de las Américas Puebla, Escuela de Ciencias Sociales, Artes y Humanidades, 2006, 64 páginas *(*Licenciatura en Relaciones Internacionales),
- Ortega Zacarías Roberto, *La importancia geopolítica de los servicios de inteligencia civiles como instrumento de política exterior: el caso del Centro de Investigación y Seguridad Nacional (2000-2012)*, México, UNAM, Facultad de Estudios Superiores Aragón, enero 2013, 73 páginas. (Licenciatura Relaciones Internacionales, Asesor Villavicencio López Rodolfo)

7.4 Fuentes consultadas

- About CIA, Center of Intelligence Agency, [en línea], Dirección URL:https://www.cia.gov/about-cia
- Abrams Elliot, *Dictators, Democracies, and Wikileaks,* [en línea], Wall Street Journal, 1 de diciembre 2010, Dirección URL: http://www.cfr.org/media-and-foreign-policy/dictators-democracies-wikileaks/p23542
- Ackerman Spencer, *Snowden leak shines light on US intelligence agencies' use of contractors*, [en línea], The Guardian, 10 de junio 2013, Dirección URL:http://www.theguardian.com/world/2013/jun/10/edward-snowden-booz-allen-hamilton-contractors
- Adams, James. "Virtual Defense", [en línea], Foreign Affairs, Num. 3, Vol. 80, (May - Jun 2001), Pp. 98-112, Dirección URL:http://www.studentpulse.com/articles/627/cyber-terrorism-and-ir-theory-realism-liberalism-and-constructivism-in-the-new-security-threat
- AF*P, Obama anuncia el fin de espionaje a aliados, [en* línea], México, El economista, *17 de enero 2014,* Dirección URL:http://eleconomista.com.mx/internacional/2014/01/17/obama-anuncia-fin-espionaje-aliados
- AFP, *El casi desconocido artículo 702 que permite a EE.UU. espiar a internet*, [en línea], El País, 11 de junio 2013, Dirección URL: http://www.elpais.com.uy/mundo/articulo-eeuu-epiar-internet.html
- Amnistía Internacional España, *Wikileaks y la libertad de expresión. Preguntas y respuestas,* [en línea], Amnistía Internacional, 9 de diciembre de 2010, Dirección RL:https://www.es.amnesty.org/noticias/noticias/articulo/wikileaks-y-la-libertad-de-expresion-preguntas-y-respuestas/
- Andrew Lewis James, *Simple Tests for Surveillance*, [en línea], Center for Strategic & International Studies (CSIS), 12 de Junio 2013, Dirección URL: https://csis.org/publication/simple-tests-surveillance, [Consultado el 7 de octubre de 2013].

- AP, *Espionaje, medida para proteger a EU: NSA,* [en línea], México, El Universal, 11 de diciembre 2013, Dirección URL:http://www.eluniversal.com.mx/el-mundo/2013/espionaje-medida-para-proteger-a-eu-nsa-972345.html
- AP, *Wikileaks: Alemania y EEUU planean programa de espionaje satelital,* [en línea], La tercera.com, 3 de enero de 2011, Dirección URL:http://www.latercera.com/noticia/mundo/2011/01/678-335275-9-wikileaks-alemania-y-eeuu-planean-programa-de-espionaje-satelital.shtml
- Ball James, *Wikileaks cables paint chequered picture of Ecuador,* [en línea], The Guardian, 19 de junio 2012, Dirección URL:http://www.theguardian.com/world/2012/jun/19/wikileaks-cables-ecuador-julian-assange
- *Bartlett Manuel, Sumisión intolerable,* [en línea], *El Universal, 16 de diciembre de 2010,* Dirección URL: http://www.eluniversal.com.mx/editoriales/50993.html
- Barón Ana, *Para EE.UU., la relación bilateral está teñida de política interna*, [en línea], El Clarín, Argentina, 6 de marzo de 2011, Dirección URL: http://www.clarin.com/politica/EEUU-relacion-bilateral-politica-interna_0_439156142.html
- BBC Mundo, *Wikileaks: la preocupación china por controlar internet*, [en línea], BBC Mundo, 5 de diciembre 2010, Dirección URL:http://www.bbc.co.uk/mundo/noticias/2010/12/101205_wikileaks_eeuu_china_internet_google_ciberataque_jp.shtml
- Bill Keller, *Wikileaks, epílogo*, [en línea], El País, 21 de febrero 2012, Dirección URL: http://internacional.elpais.com/internacional/2012/02/20/actualidad/1329771586_792156.html
- Bill Dedman, *U.S. v. WikiLeaks: espionage and the First Amendment*, [en línea], NBC News, Dirección URL:http://www.nbcnews.com/id/40653249/#.UowdEtJFWSo

- Bloomfield Aubrey, *Booz Allen Hamilton : 70 % of the U.S. Intelligence Budget Goes to Private Contractors*, [en línea], PolicyMic, Dirección URL:http://www.policymic.com/articles/48845/booz-allen-hamilton-70-of-the-u-s-intelligence-budget-goes-to-private-contractorsBazan Elizabeth, *The Foreign Intelligence Surveillance Act: An Overview of the Statutory Framework and U.S. Foreign Intelligence Surveillance Court and U.S. Foreign Intelligence Surveillance Court of Review Decisions*, Congressional Research Service, 15 febrero 2007, [en línea], Dirección URL:http://www.fas.org/sgp/crs/intel/RL30465.pdf
- Bloomfield Aubrey, *Booz Allen Hamilton : 70 % of the U.S. Intelligence Budget Goes to Private Contractors*, [en línea], PolicyMic, Dirección URL:http://www.policymic.com/articles/48845/booz-allen-hamilton-70-of-the-u-s-intelligence-budget-goes-to-private-contractors
- Borja M., *Análisis de la Ley Patriota de los Estados Unidos y su repercusión en el ámbito internacional*, Mens Iuris, 29 de marzo 2012, [en línea], Dirección URL:http://mensiuris.wordpress.com/2012/03/29/analisis-de-la-ley-patriota-de-los-estados-unidos-y-su-repercusion-en-el-ambito-internacional/
- Born Hans y Caparini Marina, Democratic Control of Intelligence Service: Containing Rogue Elephants, Gran Bretaña, Ed. Ashgate Publishing Company, 2007, p. 18, [en línea], Dirección URL: http://books.google.com.mx/books?id=FeGhAgAAQBAJ&pg=PA18&lpg=PA18&dq=intelligence+agencies+out+of+control&source=bl&ots=_jOMsbAOiX&sig=7ofbt8IGXVlXx1_BmrC1e8YVzU8&hl=es&sa=X&ei=lUUGVIWME4y-ggSWtICwCg&ved=0CFQQ6AEwBDgK#v=onepage&q=intelligence%20agencies%20out%20of%20control&f=false
- Bosker Bianca, *Internet 'Kill Switch' Approved By Senate Homeland Security Committee*, Huffington Post, Estados Unidos, 25 de junio de 2010, [en línea], Dirección

URL:http://www.huffingtonpost.com/2010/06/25/internet-kill-switch-appr_n_625856.html

- Burghardt Tom, *ECHELON Today: The Evolution of an NSA Black Program*, [en línea], Global Reserch, Julio 2013, Dirección URL: http://www.globalresearch.ca/echelon-today-the-evolution-of-an-nsa-black-program/5342646
- Burtseva Larisa, Tyrsa Valentyn, Flores Ríos Brenda Leticia, *Norbert Wiener: Padre de la cibernética*, [en línea], UABC, Mexicali, Abril-Junio 2006, Dirección URL: 132.248.129.5/cursoOJS/index.php/uabc/article/download/857/863, [Consultado el 24 de noviembre 2013].
- Cable 07MEXICO1068, ANTI-DRUG OPS EXTENDED TO EIGHT STATES, Embajada de México, 2 de marzo 2007, Dirección URL:http://www.wikileaks.ch/cable/2007/03/07MEXICO1068.html
- Cable 06MEXICO6481, Embajada de Estados Unidos en México, Las deficiencias políticas de Fox, significativas, 15 de noviembre 2006, Dirección UR:http://wikileaks.jornada.com.mx/cables/gobierno-de-vicente-fox/06mexico6481/#sthash.ENc5YNvm.dpuf
- Cable 09STATE124636, Secretaría de Estado, Clinton pide informe sobre Calderón, 4 de diciembre 2009, Dirección URL: http://wikileaks.jornada.com.mx/cables/gobierno-felipe-calderon/09state124636/#sthash.ce87cOSn.dpuf
- Cable 09MEXICO1055, Embajada de Estados Unidos en México Serias consecuencias, si Calderón no logra contener el crimen, 14 de abril 2009, Dirección URL:http://wikileaks.jornada.com.mx/cables/gobierno-felipe-calderon/09mexico1055/#sthash.kbQWQ5GP.dpuf
- Cable 10MEXICO83, Embajada de Estados Unidos en México, Existe descoordinación entre agencias de seguridad, 29 de enero de 2010, Dirección URL: http://wikileaks.jornada.com.mx/cables/narcotrafico/existe-

descoordinacion-entre-agencias-de-seguridad-cable-10mexico83/#sthash.MiJ9YqVO.dpuf

- Cable 09STATE132349, Secretaría de Estado, Argentina: Kirchner interpersonal, 31 de diciembre 2009, Dirección URL:http://www.wikileaks.ch/cable/2009/12/09STATE132349.html
- Cable 06BUENOSAIRES1462, Embajada de Estados Unidos en Buenos Aires, Argentina: The K-style of politics
- Cable 09BEIJING3128, Embajada de Beijing, Portrait of Vice President Xi Jinping: "Ambitious Survivor" of the Cultural Revolution, 16 de noviembre de 2011, Dirección URL: http://internacional.elpais.com/internacional/2010/12/28/actualidad/1293490818_850215.html
- Cable 08STATE43817, Secretary of State, Syria's Clandestine nuclear program, 25 de abril 2008, Dirección URL: http://internacional.elpais.com/internacional/2010/12/26/actualidad/1293318008_850215.html
- Cable 08NAPLES118, Consulado de Napoles, Organized Crime III: Confronting Organized Crime in Southern Italy, 6 de junio 2008, Dirección URL:http://internacional. elpais.com/internacional/2011/01/07/actualidad/1294354804_850215.html
- Cable 09ROME1187, Embajada de Roma, Italy: Scandals taking toll on Berlusconi's personal and political health, 27 octubre 2009, Confidential, Dirección URL:http://www.cablegatesearch.net/cable.php?id=09ROME1187
- Cables 09ROME97, Embajada de Roma, Italy-Russia relations: The view from Rome, 26 de enero de 2009, SECRETO, Dirección URL: http://www.cablegatesearch.net/cable.php?id=09ROME97
- Calabresi Massimo, *Wikileaks'War on Secrecy: Truth' consequences*, [en línea], TIME Magazine, 2 de diciembre 2010, http://content.time.com/time/magazine/article/0,9171,2034488,00.html

- Caro Bejarano Ma. José, *De la ciberseguridad en la Seguridad Nacional,* [en línea], España, Instituto Español de Estudios Estratégicos, Núm. 78, 27 de diciembre de 2012, Dirección URL:http://www.ieee.es/Galerias/fichero/docs_informativos/2012/DIEEEI78-2012_EvolucionCiberseguridad_MJCB.pdf
- Carozo Blumsztein Eduardo, *Sistemas SCADA, consideraciones de seguridad,* [en línea], México, Revista Seguridad, 16 de julio de 2013, Dirección URL:http://revista.seguridad.unam.mx/numero-18/sistemas-scada-consideraciones-de-seguridad
- Carr David, *Is this the WikiEnd?*, [en línea], The New York Times, 6 de noviembre 2011, Dirección URL:http://query.nytimes.com/gst/fullpage.html?res=9B03E1DF153FF935A35752C1A9679D8B63
- Chabrow Erick, *Obama Issues Cybersecurity Executive Order*, [en línea], Estados Unidos, Gov Info Security, Febrero 2013, Dirección URL:http://www.govinfosecurity.com/obama-issues-cybersecurity-executive-order-a-5506
- Chabrow Erick, *Cybersecurity Legislation: What's Next?*, [en línea], Estados Unidos, Gov Info Security, septiembre 2013, Dirección URL: http://www.govinfosecurity.com/cybersecurity-legislation-whats-next-a-6063
- CIA, *Historia de la CIA*, [en línea], Central Intelligence Agency, Dirección URL: https://www.cia.gov/es/about-cia/history-of-the-cia
- CIA, *George Bush Intelligence Center*, [en línea], Estados Unidos, CIA, Dirección URL:https://www.cia.gov/about-cia/todays-cia/george-bush-center-for-intelligence, [Consultado el 21 de marzo de 2014].
- Chivers C. J., et.al., *View is bleaker than official portrayal of War in Afghanistan*, [en línea], The New York Times, 25 de Julio de 2010, Dirección URL: http://www.nytimes.com/2010/07/26/world/asia/26warlogs.html

- CNN en México, *EU busca explotar alianzas contra Italia, pese al declive del país: WikiLeak,* [en línea], CNN México, 18 de febrero de 2011, Dirección URL: http://mexico.cnn.com/mundo/2011/02/18/eu-busca-explotar-alianza-con-italia-pese-al-declive-del-pais-wikileaks
- CNN Wire Staff, *Clinton condemns leak as 'attack on international community'*, [en línea], CNN U.S., 30 de noviembre 2010, Dirección URL: http://www.cnn.com/2010/US/11/29/wikileaks/
- Convenio de Ciberdelincuencia del Consejo de Europa, Enciclopedia Jurídica, Dirección URL:http://www.inteco.es/wikiAction/Seguridad/Observatorio/area_juridica_seguridad/Enciclopedia/Articulos_1/convenio_ciberdelincuencia_del_consejo_europa
- Convenio sobre la Ciberdelincuencia, [en línea], Dirección URL:http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Convention%20and%20protocol/ETS_185_spanish.PDF
- Corrin Amber, *Is FISMA why NSA influenced NIST?,* [en línea], Revista FCW, 1 de octubre de 2013, Dirección URL:http://fcw.com/articles/2013/10/01/fisma-nist-nsa.aspx
- Davies Nick, *Afghanistan war logs: Masive leak of secret files exposes truth of occupation*, [en línea], The Guardian, 25 de Julio 2010, Dirección URL:http://www.theguardian.com/world/2010/jul/25/afghanistan-war-logs-military-leaks
- Deans Jason, "Julian Assange wins Martha Gellhorn journalism prize." [en linea], *The Guardian, 2 de junio 2011, Dirección URL:* http://www.theguardian.com/media/2011/jun/02/julian-assange-martha-gelhorn-prize
- *Declaración Universal de los Derechos Humanos*, [en línea], CINU, Dirección URL:http://www.cinu.mx/onu/documentos/declaracion-universal-de-los-d/

- De Castro Lozano Carlos, *Introducción a SCADA, UCO,* [en línea], Dirección URL:http://www.uco.es/grupos/eatco/automatica/ihm/descargar/scada.pdf
- De Cordoba Jose, *U.S. Ambassador to Mexico Resigns Following WikiLeak Flap*, [en línea], Wall Street Journal, (Mar. 19, 2011), Dirección URL:http://online.wsj.com/article/SB10001424052748704021504576211282543444242.html
- De Santiago Freda Manuel, *Wikileaks, periodismo y trasparencia: los filtros de las filtraciones*, [en línea], Derecom, Dirección URL: http://derecom.com/numeros/pdf/wikileaks.pdf.
- Dedman Bill, U.S. v. WikiLeaks: espionaje and the First Amendment, NBC News, Dirección URL:http://www.nbcnews.com/id/40653249/#.UowdEtJFWSo.
- Deibert Ron, *The Post-Cablegate Era*, [en línea], Estados Unidos, The New York Times, 11 de diciembre 2010, Dirección URL: http://www.nytimes.com/roomfordebate/2010/12/09/what-has-wikileaks-started/after-wikileaks-a-new-era
- Department of Justice ,*The USA PATRIOT Act: Preserving Life and Liberty*, [en línea], Estados Unidos, Department of Justice, Dirección URL: http://www.justice.gov/archive/ll/highlights.htm
- Department of State*, National Security Act of 1947*, [en línea], Estados Unidos, Department of State, Office of the Historian, Dirección URL:http://history.state.gov/milestones/1945-1952/national-security-act
- Department State, *Information Sharing in the Era of WikiLeaks: Balancing Security and Collaboration*, [en línea], Estados Unidos, Department State, Dirección URL:http://www.state.gov/m/rls/remarks/2011/158400.htm
- Department of Defense, *Information and Cyberspace Issue Paper No. 1: information as an Element to Combat Power*, [en línea], Estados Unidos, Departamento de Defensa, 21 febrero 2008, Pp. 6, Dirección URL: http://www.defense.gov/Blog_files/Blog_assets/20080408_ColParks_issuepaper.pdf

- Department of Defense, *US. Cyber Command Fact Sheet*, [en línea], Estados Unidos, US Department of Defense, 25 de mayo de 2010, Dirección URL:http://www.defense.gov/home/features/2010/0410_cybersec/docs/CYberFactSheet%20UPDATED%20replaces%20May%2021%20Fact%20Sheet.pdf
- DHS, *About US*, [en línea], Estados Unidos, US-CERT, Dirección URL:http://www.us-cert.gov/about-us
- *DHS, Federal Information Security Management Act (FISMA)*, [en línea], Estados Unidos, Departarment of Home Security, Dirección URL:https://www.dhs.gov/federal-information-security-management-act-fisma
- EFE, Supremo de EU rechaza revisar programas de espionaje, [en línea], México, El Universal, 18 noviembre 2013, Dirección URL:http://www.eluniversal.com.mx/el-mundo/2013/espionaje-eu-snowden-966426.html
- El Universal, Perfil *Carlos Pascual, de Stanford y de Harvard a México,* [en línea], El Universal, 26 de marzo de 2009, Dirección URL:http://www.eluniversal.com.mx/notas/586468.html Los cables que Wikileaks filtró sobre Ecuador, BBC Mundo, 20 de junio 2012, Dirección URL:http://www.bbc.co.uk/mundo/noticias/2012/06/120620_ecuador_wikileaks_assange_correa_cables_pea.shtml
- Elola Joseba; De Cózar Álvaro; Monge Yolanda, *La verdad sobre el Cablegate*, [en linea], España, El País, 4 diciembre 2010, Dirección URL: http://internacional.elpais.com/internacional/2010/12/04/actualidad/1291417217_850215.html
- EFE, *Unos cables de WikiLeaks describen un Ejército egipcio dividido en fracciones,* [en línea], 20 minutos, es, 5 de febrero 2011, Dirección URL:http://www.20minutos.es/noticia/950658/0/wikileaks/ejercito/egipto/

- EFE,*Obama anunció cambios a la política de espionaje de la NSA*, [en línea], Univision Noticias, 17 de enero de 2014, Dirección URL:http://noticias.univision.com/article/1819820/2014-01-17/estados-unidos/noticias/obama-anunciara-cambios-en-la-nsa
- Eriksson Johan y Giacomello Giampiero, "Information Revolution, Security, and International Relations; (IR) relevant Theory?", [en línea], *International Political Science Review,* Ed. Sage Publications, Núm. 3, Vol. 27, 2006, Pp. 221-244. Dirección URL:http://myweb.rollins.edu/tlairson/pek/inforevintrela.pdf
- Evans Rob; Harding Luke; Hooper John, *WikiLeaks cables: Berlusconi' profited from secret deals' with Putin,* [en línea], The Guardian, 2 de diciembre 2010, Dirección URL:http://www.theguardian.com/world/2010/dec/02/wikileaks-cables-berlusconi-putin
- FAS, *Intelligence Budget Data*, Estados Unidos, [en línea], Dirección URL: http://www.fas.org/irp/budget/index.html?PHPSESSID=70809e6b347db7b2122df1ef24d743e0
- Firestone David, *Why are the Intelligence Budgets a State Secret?,* [en línea], Estados Unidos, The New York Times, 17 de enero de 2014, [en línea], Dirección URL:http://takingnote.blogs.nytimes.com/2014/01/17/why-are-the-intelligence-budgets-a-state-secret/?ref=centralintelligenceagency
- Fenster Mark, *Disclosure's Effects: WikiLeaks and Transparency*, [en línea], Revista Iowa Law Review, Universidad de Iowa, Vol. 97:753, 2012, Pp. 754-807, Dirección URL:http://www.uiowa.edu/~ilr/issues/ILR_97-3_Fenster.pdf,
- Fojón Enrique; Sanz Ángel, *Ciberseguridad en España: una propuesta para su gestión,* [en línea], España, Análisis del Real Instituto Elcano, ARI Núm. 101/2010, 18 de junio 2010, Dirección URL:http://www.realinstitutoelcano.org/wps/wcm/connect/c1360e8042e4fcf49e51ff5cb2335b49/ARI102-

2010_Fojon_Sanz_ciberseguridad_Espana.pdf?MOD=AJPERES&CACHEID=c1360e8042e4fcf49e51ff5cb2335b49

- Foro e-Gobierno OEA, Boletín electrónico, Dirección URL:http://www.suboletin.com/contentsoea/docs/Boletin_58/Paratenerencuenta58.htm
- Forest James J. F., *Countering Terrorism and insurgency in the 21st Century*, Estados Unidos, Ed. Praeger Security International,2007, p. 421, [en línea], Dirección URL: http://books.google.com.mx/books?id=RMUVEw1nfSUC&pg=PA421&dq=intelligence+agencies+definition&hl=es&sa=X&ei=B8EHVMXiB43IggSjsIKIBA&ved=0CCQQ6AEwAQ#v=onepage&q=intelligence%20agencies%20definition&f=false,
- Fung Brian, *U.S. intelligence agencies can't justify why they use so many contractors,* [en línea], Washington Post, 14 de febrero 2014, Dirección URL:http://www.washingtonpost.com/blogs/the-switch/wp/2014/02/14/u-s-intelligence-agencies-cant-justify-why-they-use-so-many-contractors/
- Fung Brian, *Are Obama's new cybersecurity standards a form of privacy regulation in disguise?,* [en línea], Estados Unidos, The Washington Post, 11 de octubre 2013, Dirección URL:http://www.washingtonpost.com/blogs/the-switch/wp/2013/10/11/are-obamas-new-cybersecurity-standards-a-form-of-privacy-regulation-in-disguise/
- Gelb Leslie H., *Wikileaks accidentally helps U.S.*, [en línea], The Daily Beast, 20 de noviembre 2010, http://www.thedailybeast.com/articles/2010/11/30/wikileaks-helps-america-how-julian-assange-proved-us-working-hard-on-policy-problems.html?cid=hp:mainpromo4
- Gellman Barton y Miller Greg, EU tiene presupuesto Negro para espionaje, El Economista, 28 de agosto 2013, Dirección

URL:http://eleconomista.com.mx/internacional/2013/08/29/estados-unidos-tiene-presupuesto-negro-espionaje

- Glenn Hastedt, *Evaluating Congressional Oversight of Intelligence*, [en línea], E-International Relatons, 23 de agosto 2013, Dirección URL:http://www.e-ir.info/2013/08/23/evaluating-congressional-oversight-of-intelligence/
- Gómez de Ágreda Ángel, *El ciberespacio como entorno social y de conflicto,* [en línea], España, Instituto Español de Estudios Estratégicos, Num.17, 21 de febrero de 2012, Dirección URL: http://www.ieee.es/Galerias/fichero/docs_opinion/2012/DIEEEO17_CiberespacioConflicto_Agreda.pdf
- Graf Alan, Guerra y represión: la 'USA-Patriot Act' recorta los derechos civiles y ataca las libertades fundamentales en EEUU so pretexto de garantizar la "seguridad nacional", [en línea], 17 de mayo 2010, Dirección URL:http://www.avizora.com/atajo/informes/usa_textos/usa_textos_2/0037_ley_patriotica.htm
- Halchin Elaine; Kaiser Frederick M., *Congressional Oversight of Intelligence: Current Structure and Alternatives*, [en línea], Congressional Research Service, 14 mayo 2012, Dirección URL: http://www.fas.org/sgp/crs/intel/RL32525.pdf
- Halliday Josh, *WikiLeaks: US advised to sabotage Iran nuclear sites by German thinktank,* [en línea], The Guardian, 18 de enero de 2010, Dirección URL:http://www.theguardian.com/world/2011/jan/18/wikileaks-us-embassy-cable-iran-nuclear
- Hass Richard N, *Richard Haass on the Lessons of WikiLeaks,* [en línea], Newsweek, 12 de abril 2010, Dirección URL: http://www.newsweek.com/richard-haass-lessons-wikileaks-68889?from=rss
- Hernández Jaime J., *El 11-S y los programas de espionaje estadounidenses,* [en línea], México, El Universal, 9 septiembre 2013,

Dirección URL:http://www.eluniversal.com.mx/el-mundo/2013/impreso/el-11-s-y-los-programas-de-espionaje-estadounidenses-84033.html

- Hirst Joel D., *Cablegates: Obama's Diplomatic Waterloo*, [en línea], Huffington Post, Dirección URL:http://www.huffingtonpost.com/joel-d-hirst/cablegate-obamas-diplomat_b_792303.html?view=print
- Hooper John, *Silvio Berlusconi's health hit by party lifestyle, WikiLeaks cable says*, [en línea], The Guardian, 2 de diciembre 2010, Dirección URL:http://www.theguardian.com/world/2010/dec/02/silvio-berlusconi-health-party-wikileaks?guni=Article:in%20body%20link
- Hoover Nicholas, *Homeland Security, Defense Sign Cybersecurity Pact*, [en línea], Information Week Government, 14 de octubre 2010, Dirección URL: http://www.informationweek.com/government/security/homeland-security-defense-sign-cybersecu/227800034
- Ignatius David, *Bipartisanship in Congress should start with intelligence oversight,* [en línea], Washington Post, 5 de diciembre 2010, Dirección URL:http://www.washingtonpost.com/wp-dyn/content/article/2010/12/03/AR2010120304304.html
- Jackson William, *Eisntein 3 goes live with automated malware blocking*, [en línea], GCN, 24 de Julio 2013, Dirección URL: http://gcn.com/articles/2013/07/24/einstein-3-automated-malware-blocking.aspx
- Jakobsen Jo, *Relations-Kenneth Waltz,* [en línea], Popular Social Science, Dirección URL: http://www.popularsocialscience.com/2013/11/06/neorealism-in-international-relations-kenneth-waltz/
- Johnson Toni, *Wikileaks and Challenges to Internet freedom,* [en línea], Council of Foreign Relations, Entrevista a Adan Segal, 17 de diciembre 2013, Dirección URL:http://www.cfr.org/internet-policy/wikileaks-challenges-internet-freedom/p23661

- Kean Thomas H.; “Lee H. Hamilton, *Testimony, US Senate Committee on Commerce, 111 Congress, 20 de enero 2010”, en Halchin Elaine y Kaiser Frederick M., Congressional Oversight of Intelligence: Current Structure and Alternatives*, [en línea], Congressional Research Service, 14 mayo 2012, p.3, Dirección URL: http://www.fas.org/sgp/crs/intel/RL32525.pdf
- Kelley Michael, *Top Secret US Intelligence ‘Black Budget’ published for first time after being leaked by Snowden,* [en línea], Business Insider, 29 de agosto 2013, Dirección URL:http://www.businessinsider.com/us-intelligence-communitys-top-secret-black-budget-2013-8
- Kinsman Jeremy, *Truth and consequence: The Wikileaks saga*, [en línea], Policy Options, Febrero 2011, Dirección URL:http://www.irpp.org/en/po/from-climate-change-to-clean-energy/truth-and-consequence-the-wikileaks-saga/
- Kroenig Matthew; Pavel Barry, *How to deter terrorism*, [en línea], Estados Unidos, The Washington Quarterly, 2012, Dirección URL: http://csis.org/files/publication/TWQ_12Spring_Kroenig_Pavel.pdf
- Leed Maren, *Offensive Cyber Capabilities at the Operational Level*, [en línea], CSIS, 16 de septiembre 2013, Dirección URL:https://csis.org/publication/offensive-cyber-capabilities-operational-level
- Lewis James Andrew, *Simple Tests for Surveillance*, [en linea], Center for Strategic & International Studies (CSIS), 12 de Junio 2013, Dirección URL: https://csis.org/publication/simple-tests-surveillance
- Levine Adam, *Previous Wikileaks release forced tighter security for U.S. military,* [en línea], CNN U.S., 30 de noviembre 2010,Dirección URL:http://www.cnn.com/2010/US/11/28/wikileaks.security/
- Lewis James Andrew, *Private Retaliation in Cyberspace*, [en línea], CSIS, 22 de mayo 2013, Dirección URL:https://csis.org/publication/private-retaliation-cyberspace
- Libicki Martin C., *Don't Buy the Cyberhype,* [en línea], Foreign Affairs, 14 de agosto 2013, Dirección

URL:http://www.foreignaffairs.com/articles/139819/martin-c-libicki/dont-buy-the-cyberhype

- Lindsay James M., *Anglo-U.S. Relations can overcome Wikileaks fallout, Council on Foreign Relations*, [en línea], 2 de diciembre 2010, Dirección URL:http://blogs.cfr.org/lindsay/2010/12/03/anglo-u-s-relations-can-overcome-wikileaks-fallout/
- Lister Tim, *El presidente de Egipto sigue siendo un aliado vital de EU, dice WikiLeaks*, [en línea], CNN México, 28 de enero de 2011, Dirección URL: http://mexico.cnn.com/mundo/2011/01/28/el-presidente-de-egipto-sigue-siendo-un-aliado-vital-de-eu-dice-wikileaks,
- Lister Tim, *WikiLeaks revela disputa entre Francia y Alemania por tecnología satelital*, [en línea], CNN México, 3 de enero 2011, Dirección URL: http://mexico.cnn.com/mundo/2011/01/03/wikileaks-revela-disputa-entre-francia-y-alemania-por-tecnologia-satelital
- Loreti Damián y Lozano Luis, *El caso Wikileaks y su relación con el derecho a la información*, [en línea], Catedra, Dirección URL:http://www.catedras.fsoc.uba.ar/loreti/documentos_de_la_catedra/wikileaksdali.pdf
- MacAskil Ewen; Watts Jonathan, *US intelligence spending has doubled since 9/11, top secret budget reveals,* [en línea], The Guardian, 29 de agosto 2013, Dirección URL:http://www.theguardian.com/world/2013/aug/29/us-intelligence-spending-double-9-11-secret-budget
- Markey Daniel S., *Will Wikileaks hobble U.S. Diplomacy?,* [en línea], Council on Foreing Relations, 1 de diciembre 2010, Dirección URL:http://www.cfr.org/diplomacy-and-statecraft/wikileaks-hobble-us-diplomacy/p23526
- Marsh Taylor, *WikiLeaks Blowback in the Era of Zuckerberg,* [en línea], Huff Post, 30 de noviembre de 2010, Dirección URL: http://www.huffingtonpost.com/taylor-marsh/wikileaks-blowback-in-the_b_789911.html

- Masters Jonathan, *Confronting Cyber Threat*, [en línea], Council on Foreign Relations, 23 de mayo 2011, Dirección URL:http://www.cfr.org/technology-and-foreign-policy/confronting-cyber-threat/p15577
- Masters Jonathan, *Confronting the Cyber Threat*, [en línea], Estados Unidos, Council of Foreing Relations, 23 de mayo 2013, Dirección URL: http://www.cfr.org/technology-and-foreign-policy/confronting-cyber-threat/p15577
- McDonoug Denis; Rudman Mara; Rundlet Peter, *No Mere Oversight Congressional Oversight of Intentelligence is Broken,* [en línea], Center for American Progress, Junio 2006, Dirección URL:http://www.americanprogress.org/kf/NOMEREOVERSIGHT.PDF
- McAndrew Tom, *FISMA vs. FedRAMP*, [en línea], Estados Unidos, Coalfire, Abril 2012, Dirección
- URL:http://www.coalfire.com/medialib/assets/PDFs/Perspectives/Coalfire-Perspective-FISMA-vs-FedRAMP.pdf
- McAuliff Michael, *NSA Surveillance largely defended by Congress in rare public hearing,* [en línea], Huffington Post, 18 de junio 2013, Dirección URL:http://www.huffingtonpost.com/2013/06/18/nsa-surveillance-congress_n_3461346.html
- Mena Erazo Paúl, Ecuador y EE.UU. en nuevo roce bilateral, [en línea], BBC Mundo, 5 de abril 2011, Dirección URL: http://www.bbc.co.uk/mundo/noticias/2011/04/110405_ecuador_eeuu_embajadora_lr.shtml, [Consultado el 10 de agosto de 2014].
- Miller Greg; O'Keefe Ed; Goldman Adam, *La CIA hackeó al Comité de Inteligencia: Dianne Feinstein*, [en línea], México, El Economista, 11 de marzo 2014, Dirección URL: http://eleconomista.com.mx/internacional/2014/03/11/cia-hackeo-comite-inteligencia-dianne-feinstein
- Ministerio de Defensa de España, *Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio. Cuadernos de Estrategia*, [en línea],

España, , Ministerio de Defensa de España, Febrero 2011, 368 páginas, Dirección URL:http://www.bibliotecavirtualdefensa.es/BVMDefensa/i18n/catalogo_imagenes/grupo.cmd?path=17029

- Moore Tristana, *German-U.S. Relations Will Survive WikiLeaks — but the Trust Is Gone,* [en línea], Time World, 29 de noviembre 2010, Dirección URL: http://content.time.com/time/world/article/0,8599,2033526,00.html
- Nacht Michael, *The cyber security challenge*, [en línea], Estados Unidos,The Berkeley Blog, 6 octubre de 2013, Dirección URL:http://blogs.berkeley.edu/2013/06/10/the-cyber-security-challenge/
- Nakashima Ellen, *Bush Order Expands Network Monitoring*, [en línea], Estados Unidos, Washington Post, 26 de enero 2008, Dirección URL:http://www.washingtonpost.com/wp-dyn/content/article/2008/01/25/AR2008012503261.html
- Nakashima Ellen, *U.S. cybersecurity plans lagging, critics say*, [en línea], Estados Unidos, The Washington Post, 16 de septiembre 2010, Dirección URL:http://www.washingtonpost.com/wp-dyn/content/article/2010/09/16/AR2010091603281.html
- National Institute of Standards and Technology, [en línea], Dirección URL:http://www.nist.gov/,
- Noelle-Neumann Elisabeth, “La espiral del silencio. La opinión pública y los efectos de los medios de comunicación”, *Revista Comunication & Society*, Universidad de Navarra, Núm. 1. Vol. VI, 1993, Dirección URL: http://www.unav.es/fcom/comunicacionysociedad/es/articulo.php?art_id=226
- Notimex, *Revelan espionaje de EUA y Reino Unido a Italia,* [en línea], México, El Universal, 24 de octubre 2013, Dirección URL:http://www.eluniversal.com.mx/el-mundo/2013/espionaje-eu-italia-960534.html

- Notimex Berlin, *Niega Alemania que filtraciones de Wikileaks afecten relación con EU,* [en línea], Crónica.com, 29 de noviembre 2010, Dirección URL:http://www.cronica.com.mx/especial.php?id_nota=546947&id_tema=1434
- O'Donnell Santiago, ArgenLeaks, Buenos Aires, Ed. Ramdom House Mondadori, S.A., 2011, [en línea] Dirección URL: http://books.google.com.mx/books?id=fA3c1tEgaF4C&printsec=frontcover&dq=wikileaks&hl=es&sa=X&ei=BYbyU5iNKcPR8AGO5oHgCg&ved=0CEQQ6AEwBQ#v=onepage&q=wikileaks&f=false
- Orozco Gabriel, "El concepto de seguridad en la Teoría de las Relaciones Internacionales", [en línea], España, *Revista CIDOB d' Afers Internacionals*, Núm.72, pp. 161-180, Dirección URL: http://www.raco.cat/index.php/revistacidob/article/viewFile/28455/28289
- Oswald Spring Úrsula y Gunter Brauch Hans, *Reconceptualizar la seguridad en el siglo XXI, [en línea]*, México, UNAM, 2009, pp. 283, Dirección URL: http://www.crim.unam.mx/drupal/?q=node/407
- Peterson Andrea y Pool Sean, *U.S. Cybersecurity Policy in Context*, [en línea], Center for American Progress, 22 de febrero 2013, Dirección URL: http://www.americanprogress.org/issues/technology/news/2013/02/22/54418/u-s-cybersecurity-policy-in-context/
- Presidency US, *Statement of Administration Policy Cyber Security Research and Development Act*, [en línea], Estados Unidos, The American Presidency Project, 5 de febrero 2002, Dirección URL:http://www.presidency.ucsb.edu/ws/?pid=24622
- Piras Annalisa, *Wikileaks cables portrait of Silvio Berlusconi is a worry beyond Italy,* [en línea], The Guardian, 3 de diciembre 2010, Dirección URL: http://www.theguardian.com/commentisfree/2010/dec/03/wikileaks-cables-silvio-berlusconi
- Priest Dana y Arkin William M., *National Security Inc*., [en línea], Washington Post Investigation, Dirección

URL:http://projects.washingtonpost.com/top-secret-america/articles/national-security-inc/

- Radó Nóra, *On WikiLeaks and Diplomacy: Secrecy and Trasparency in the Digital Age*, [en línea], Central European University, Department of International Relations and European Studies, Hungría (Budapest), 2011, Tesis Master en Artes, Asesor Astrov Alexander, Dirección URL: www.etd.ceu.hu/2011/rado_nora.pdf
- RAE, Definición de Ciberespacio, [en línea], Real A*cademia de la Lengua Española, Direcci*ón URL:http://lema.rae.es/drae/?val=ciberespacio
- Rain, Ottis; Lorents Peeter, *Cyberspace: Definitions and Implications*, [en línea], Estonia, Cooperativa Cyber Defence Centre of Excellence, 2010, Dirección URL: http://dumitrudumbrava.files.wordpress.com/2012/01/cyberspace-definition-and-implications.pdf
- Rebossio Alejandro y Doncel Luis, *Las revelaciones de Wikileaks sobre la presidenta Kirchner acaparan el debate político en Argentina*, [en línea], El País, Buenos Aires, 30 de noviembre 2010, Dirección URL: http://internacional.elpais.com/internacional/2010/11/30/actualidad/1291071603_850215.html
- Redacción BBC Mundo, Wikileaks: EE.UU. trata de contener el daño diplomático, [en línea], BBC Mundo, 29 de noviembre 2010, Dirección URL: http://www.bbc.co.uk/mundo/noticias/2010/11/101128_wikileaks_documentos_eeuu_cables_preocupaciones_chavez_amab.shtml?print=1
- Relatores especiales de la OEA y ONU, *Declaración Conjunta sobre Wikileaks*, [en línea], OEA, 21 de diciembre 2010, Dirección URL:http://www.oas.org/es/cidh/expresion/showarticle.asp?artID=829&lID=2
- Resolución 2625 (XXV) de la Asamblea General de Naciones Unidas, Declaración relativa a los Principios de Derecho Internacional referentes a las relaciones de amistad y a la cooperación entre los Estados de conformidad con la Carta de las Naciones Unidas, [en línea],

Dipublico.com.arg, 24 de octubre de 1970, Dirección URL: http://www.dipublico.com.ar/3971/resolucion-2625-xxv-de-la-asamblea-general-de-naciones-unidas-de-24-de-octubre-de-1970-que-contiene-la-declaracion-relativa-a-los-principios-de-derecho-internacional-referentes-a-las-relaciones-de/

- Risen James y Lichtblau Eric, *Control of Cybersecurity Becomes Divisive Issues*, [en línea], Estados Unidos, The New York Times, 16 de abril de 2009, Dirección URL:http://www.nytimes.com/2009/04/17/us/politics/17cyber.html?_r=0
- Rivera Vélez Fredy, *Inteligencia estratégica y Prospectiva*, [en línea], Ecuador, Ed. FLACSO, Mayo 2011, 296 páginas. Dirección URL: http://iaen.edu.ec/wp-content/uploads/2013/05/M.-Reyes-2011-La-inteligencia-China.-Un-acercamiento-cultural.pdf
- Rohan Brian, *U.S. sees top German diplomat arrogant: Wikileaks*, [en línea], Reuters, 28 de noviembre 2010, Dirección URL: http://www.reuters.com/article/2010/11/28/us-germany-wikileaks-idUSTRE6AR3EC20101128
- Rollins John y Henning Anna C., *Comprehensive National Cybersecurity Initiative: Legal Authorities and Policy Considerations*, [en línea], Congressional Research Service, 10 de marzo 2009, pp. 2, Dirección URL:http://www.whitehouse.gov/files/documents/cyber/Congressional%20Research%20Service%20-%20CNCI%20-%20Legal%20Authorities%20and%20Policy%20Considerations%20(March%202009).pdf
- Rosenbach Eric, *Congressional Oversight of the Intelligence Community, Belfer Center for Science and International Affairs*, [en línea], Harvard Kennedy School, julio 2009, Dirección URL:http://belfercenter.ksg.harvard.edu/publication/19146/congressional_oversight_of_the_intelligence_community.html

- Rosas María Cristina, *Ciberspacio, crimen organizado y seguridad nacional*, Etcétera, 9 de mayo 2011, [en línea], Dirección URL:http://www.etcetera.com.mx/articulo.php?articulo=7536&pag=3
- Sabbagh Dan, *WikiLeaks cables blame Chinese government for Google hacking*, [en línea], The Guardian, 4 de diciembre 2010, Dirección URL:http://www.theguardian.com/technology/2010/dec/04/wikileaks-cables-google-china-hacking
- Sanger David E., *North Korea Keeps the World Guessing*, [en línea], New York Times, 29 de noviembre 2010, Dirección URL: http://www.nytimes.com/2010/11/30/world/asia/30korea.html?pagewanted=all
- Santiago Oropeza Teresa, "Kant y su proyecto de una paz perpetua", [en línea], *Revista Digital Universitaria*, México, Ed. UNAM, Núm. 11, Vol. 5, 10 de diciembre 2004, Dirección URL: http://www.revista.unam.mx/vol.5/num11/art77/dic_art77.pdf
- Sarkesian Sam C., Williams John Allen y Cimbala Stephen J, *US National Security: Policymakers, Processes & Politics*, Estados Unidos, Ed. Lynne Rienner Publishers, 2008, 23 páginas, Dirección URL: http://issat.dcaf.ch/ser/content/download/17624/205980/file/nat%20sec%20proc%20pol%20policym.pdf.
- Schiff Adam B., *An NSA fix,* [en línea], Los Ángeles Times, 31 de octubre 2013, Dirección URL:http://www.latimes.com/opinion/commentary/la-oe-schiff-nsa-surveillance-phone-metadata--20131031,0,4107687.story#axzz2v3AJyByI
- Sehgal Ujala, *Hilary Clinton: WikiLeaks Is An "Attack On America's Foreign Policy Interests,* [en línea], Business Insider, 29 de noviembre, *Dirección URL* http://www.businessinsider.com/hilary-clinton-on-stolen-documents-2010-11#ixzz2lDXVY29C
- Shane Scott y Lehren Andrew W., *Leaked Cables Offer Raw Look at U.S. Diplomacy,* [en línea], Estados Unidos, The New York Times, 28 de

noviembre 2010, Dirección URL: http://www.nytimes.com/2010/11/29/world/29cables.html?pagewanted=1&_r=0&hp

- Shane Scott, *Spy Agencies Under Heaviest Scrutiny since abuse scandal of the '70s,* [en línea], Estados Unidos, The New York Times, 25 de julio 2013, Dirección URL: http://www.nytimes.com/2013/07/26/us/politics/challenges-to-us-intelligence-agencies-recall-senate-inquiry-of-70s.html?ref=centralintelligenceagency&_r=0
- Sheridan Mary Beth, *Calderon: WikiLeaks caused severe damage to U.S.-Mexico relations,* [en línea], Washington Post, 3 de marzo 2011, Dirección URL:http://www.washingtonpost.com/wp-dyn/content/article/2011/03/03/AR2011030302853.html
- Shorrock Tim, *Put the Spies back under one roof,* [en línea], Estados Unidos, [en línea], The New York Times, The Opinion pages, 17 de junio 2013, Dirección URL:http://www.nytimes.com/2013/06/18/opinion/put-the-spies-back-under-one-roof.html?ref=centralintelligenceagency
- Smith Cary Stacy; Hung Li-Ching, *Patriot Act, Issues and Controversies*, [en línea], Ed. Charles C. Thomas Publisher, Estados Unidos, 2010, Dirección URL:http://books.google.com.mx/books?id=7hPnSyAOeWQC&printsec=frontcover&dq=patriot+act&hl=es&sa=X&ei=WiiiUoiJMuHT2wWkn4DoBQ&sqi=2&redir_esc=y#v=onepage&q=patriot%20act&f=false
- Sottek T.C., The NSA is out of control and must be stopped, The Verger, 12 de diciembre 2013, [en línea], Dirección URL:http://www.theverge.com/2013/12/12/5200142/end-the-nsa-nightmare
- Spencer Ackerman, *Snowden leak shines light on US intelligence agencies' use of contractors,* [en línea], The Guardian, 10 de junio 2013, Dirección URL:http://www.theguardian.com/world/2013/jun/10/edward-snowden-booz-allen-hamilton-contractors
- Stark, Holger; Rosenbach Marcel, *WikiLeaks Is Annoying, But Not a Threat,* [en línea], Spiegel Online, 20 de diciembre 2010 en Päivikki Karhula, What

is the effect of Wikileaks for Freedom of Information?, [en línea], IFLA, Dirección URL:http://www.ifla.org/publications/what-is-the-effect-of-wikileaks-for-freedom-of-information

- Sturtevant Mary, *Congressional Oversight of Intelligence: One perspective*, [en línea], American Intelligence Journal, 1992, Dirección URL: http://www.fas.org/irp/eprint/sturtevant.html
- Sundby Scott E.; Pérez Cebadera María Ángeles, "Caminando sobre la cuerda floja constitucional: la USA Patriot Act" y la "Guerra contra el terror", [en línea], *Revista General de Derecho Procesal,* 15, 2008, http://repositori.uji.es/xmlui/bitstream/handle/10234/19013/29277.pdf?sequence=1
- Sutter John D., *¿Ha desatado Wikileaks la primera guerra cibernética?,* [en línea], CNN México, 12 de diciembre 2012, Dirección URL: http://mexico.cnn.com/tecnologia/2010/12/12/ha-desatado-wikileaks-la-primera-guerra-cibernetica
- Swenson Russell G. y Lemozy Susana C., *Democratización de la Función de Inteligencia*, [en línea], Estados Unidos, Ed. National Defense Intelligence College, Enero 2009, 458 páginas, Dirección URL:http://www.ni-u.edu/ni_press/pdf/Democratizaci%C3%B3n_de_la_Funci%C3%B3n_de_Inteligencia.pdf
- Tijeras Ramón, *Wikileaks, periodismo y nuevas plataformas de información*, [en línea], Comunicación 21, Número 1, Dirección URL:http://www.comunicacion21.com/de-wikileaks-a-openleaks-la-crisis-de-los-medios-y-las-nuevas-plataformas-de-informacion/Masters Jonathan, Confronting the Cyber Threat, [en línea], Council of Foreing Relations, 23 de mayo 2013, Dirección URL: http://www.cfr.org/technology-and-foreign-policy/confronting-cyber-threat/p15577

- Timm Trevor, *Cablegate One Year Later: How WikiLeaks Has Influenced Foreign Policy, Journalism, and the First Amendment*, [en línea], Electronic Frontier Foundation, 28 noviembre 2011, Dirección URL:https://www.eff.org/deeplinks/2011/11/cablegate-one-year-later-how-wikileaks-has-influenced-foreign-policy-journalism
- Tisdall Simon, *Wikileaks cables reveal China 'ready to abandon North Korea'*, [en línea], The Guardian, 29 de noviembre 2010, Dirección URL:http://www.theguardian.com/world/2010/nov/29/wikileaks-cables-china-reunified-korea,
- Tony Romm, *Intelligence Oversight has some limits in Congress*, [en línea], Político, 10 de octubre 2013, Dirección URL: http://www.politico.com/story/2013/10/intelligence-oversight-has-some-limits-in-congress-98099.html
- Traynor Ian, *WikiLeaks cables claim first scalp as German minister's aide is sacked*, [en línea], The Guardian, 3 de diciembre 2010, Dirección URL: http://www.theguardian.com/media/2010/dec/03/wikileaks-first-scalp-german-aide
- U.S Department of State, *National Security Act of 1947*, [en línea], Dirección URL:https://history.state.gov/milestones/1945-1952/national-security-act, [Consultado el 11 de marzo de 2014].
- US Military, *Secret Internet Protocol Router Network (SIPRNET),* [en línea], US MIlitary, Estados Unidos Dirección URL: http://www.usmilcom.com/military.htm
- Van Cleave Michelle K., *Counterintelligence and National Strategy*, [en línea], Ed. School for National Security Executive Education y National Defense University Press, abril 2007, Dirección URL: www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA471485
- Watson Giles, *Wikileaks Reveals Berlusconi as "Feckless", "Ineffective" and "Mouthpiece of Putin",* [en línea], Italian Life, 29 de noviembre 2010,DirecciónURL:http://www.corriere.it/International/english/articoli/2010/11/29/wikileaks-Berlusconi-leader.shtml

- *Weiland* Severin, *WikiLeaks Cables Fallout: Mole in Germany's FDP Party Comes Forward*, [en línea], Spiegel Online, 2 de diciembre 2010, Dirección URL: http://www.spiegel.de/international/germany/wikileaks-cables-fallout-mole-in-germany-s-fdp-party-comes-forward-a-732579.html
- Wikileaks, *Secret US Embassy Cables*, [en línea], Wikileaks, Dirección URL: http://wikileaks.org/cablegate.html
- Wikileaks, *What is Wikileaks?,* [en línea], Dirección URL:http://wikileaks.org/About.html
- White House, *The Comprehensive National Cybersecurity Initiative*, [en lineal], Estados Unidos, 2009, Dirección URL:http://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative
- White House, *The National Strategy to Secure Cyberspace*, [en línea], Washington, White House, February 2003, Dirección URL:http://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf
- White House, Presidente Barack Obama, [en línea], The White House, Washington, Dirección URL: http://www.whitehouse.gov/espanol/presidente-obama/
- White House, Presidentes de los Estados Unidos, [en línea], The White House, Dirección URL:http://georgewbush-whitehouse.archives.gov/president/gwbbio.es.html
- White House, *Cyber Security*, The White House, Estados Unidos, [en línea], Dirección UL: http://www.whitehouse.gov/issues/foreign-policy/cybersecurity
- White House, *Cyberspace Policy Review*, [en línea], White House, Estados Unidos, Dirección URL: http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf
- Witten Samuel, *The Effects of Wikileaks on Those Who Work at the State Department*, [en línea], Opinion Juris, Dirección

URL:http://opiniojuris.org/2010/12/18/the-effects-of-wikileaks-on-those-who-work-at-the-state-department/

- s/a, *Michael Daniel*, White House, [en línea], Dirección URL:http://www.whitehouse.gov/blog/author/Michael%20Daniel, [Consultado el 20 de febrero de 2014].
- s/a, *Obama anunció cambios a la política de espionaje de la NSA,* [en línea], Univision Noticias, 17 de enero de 2014, Dirección URL:http://noticias.univision.com/article/1819820/2014-01-17/estados-unidos/noticias/obama-anunciara-cambios-en-la-nsa
- s/a, *FISA Debate Involves More Than Terrorism*, [en línea], Daily Nexus, University of California, Santa Bárbara, 20 de febrero 2008, Dirección URL:http://web.archive.org/web/20090123213757/http://www.dailynexus.com/article.php?a=15892
- s/a, *Federal Information Security Management Act (FISMA)*, [en línea], SearchSecurity, Dirección URL:http://searchsecurity.techtarget.com/definition/Federal-Information-Security-Management-Act
- s/a, Dianne Feinstein Biography, [en línea], Dirección URL:http://www.feinstein.senate.gov/public/index.cfm/biography,
- s/a, *U.S Department of State, National Security Act of 1947*, Dirección URL:https://history.state.gov/milestones/1945-1952/national-security-act,
- s/a, Why the media (and particularly Wiki leaks) is important, Wikileak.org, Dirección URL: https://wikileaks.org/About.html,
- s/a, *FY 2013 Congressional Budget Justification,* [en línea], Estados Unidos, Washington Post, Febrero 2012, Dirección URL: http://apps.washingtonpost.com/g/page/national/inside-the-2013-us-intelligence-black-budget/420/#document/p1/a117329
- s/a, FISMA, [en línea], 2002, Dirección URL: http://csrc.nist.gov/drivers/documents/FISMA-final.pdf

- s/a, *Conexión Vital*, [en línea], México, *Revista Agora*, Núm 6, Vol. 6, 1 de julio 2013, [en línea], Dirección URL:http://agorarevista.com/es/articles/rmim/features/viewpoint/2013/07/01/feature-pr-14
- *s/a, Obama hablará sobre planes para restaurar confianza en agencias de inteligencia*, [en línea], BBC Mundo, 17 de enero de 2014, [en línea], Dirección URL:http://www.bbc.co.uk/mundo/ultimas_noticias/2014/01/140117_ultnot_obama_nsa_estados_unidos_mr.shtml
- s/a, Protecting Cyberspace as a National Asset Act of 2010, Official Summary, Open Congress, [en línea], Dirección URL:http://www.opencongress.org/bill/111-s3480/show
- s/a, *Federal Information Security Management Act*, [en línea], Estados Unidos, U.S. General Services Administration, Dirección URL:http://www.gsa.gov/portal/content/150159
- s/a, *Standars for Security Categorizations of Federal Information and Information Systems*, [en línea], Estados Unidos, Department of Commerce, 2004, Dirección URL:http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf
- s/a, *Los papeles del Departamento de Estado*, [en línea], Wikipedía, Dirección URL:http://es.wikipedia.org/wiki/WikiLeaks#Los_papeles_del_Departamento_de_Estado:_28_de_noviembre_de_2010_.28Cablegate.29
- s/a, *Preguntas y respuestas sobre los papeles del Departamento de Estado*, [en línea], Madrid, El País, 28 de noviembre de 2010, Dirección URL: http://internacional.elpais.com/internacional/2010/11/28/actualidad/1290898811_850215.html, [Consultado el 22 de octubre de 2013].
- s/a, *Leadership, Center of Intelligence Agency*, [en línea], CIA, Dirección URL: https://www.cia.gov/mobile/about-cia/leadership/index.html,

- s/a, *NSA despedirá un 90% de sus administradores de sistemas para impedir nuevas filtraciones,* [en línea], Ria Novosti, Moscú, 30 de agosto 2013, Dirección URL:http://sp.rian.ru/international/20130809/157764953.html
- *s/a, The US Embassy Cables*, [en línea], Gran Bretaña, The Guardian, Dirección URL:http://www.theguardian.com/world/the-us-embassy-cables
- s/a, *El Senado de Estados Unidos reformula la ley de seguridad informática*, [en línea], RedUsers, 1 julio 2012, Dirección URL: http://www.redusers.com/noticias/el-senado-de-estados-unidos-reformula-la-ley-de-seguridad-informatica/
- s/a, *Biografía Hans Morgenthau,* [en línea], Boletín de Relaciones Internacionales, No. 5, Agosto-Septiembre 2004, Dirección URL: http://nortecity.com.ar/relinter/numero5_pagina5.html
- s/a, *Conozca quién es Julian Assange y la cronología del caso*, [en línea], El Comercio.com, 14 Junio 2012, Dirección URL:http://www.elcomercio.com/politica/asilo-Julian-Assange-Ecuador-wikileaks-Londres-Rafael-Correa-Patino-cronologia_0_756524380.html
- s/a, *Perfil Biográfico y Académico de Norbert Wiener*, [en línea], Dirección URL: http://www.infoamerica.org/teoria/wiener1.htm
- s/a, *Inhofe wants to investigate NSA, following new report about surveillance, Intelligence World*, [en línea], Fox News, 17 de agosto 2013, Dirección URL: http://www.foxnews.com/politics/2013/08/17/inhofe-calls-for-hill-investigations-after-new-report-about-nsa-survelliance/#ixzz2cGWCrhe0
- s/a, *Mission, Nacional Security Agency & Central Security Service*, [en línea], Dirección URL:http://www.nsa.gov/about/mission/index.shtml
- s/a, *The Black Budget*, [en línea], Washington Post, Dirección URL: http://www.washingtonpost.com/wp-srv/special/national/black-budget/
- s/a, *Los Principios de Johannesburgo sobre la Seguridad Nacional, la Libertad de Expresión y el Acceso a la Información*, [en línea], Articulo 19, Noviembre 1996, Dirección URL:http://www.corteidh.or.cr/tablas/a22440.pdf

- s/a, *Who we are* , Central Intelligence Agency, [en línea], 5 de abril de 2007, Dirección URL: https://www.cia.gov/about-cia/todays-cia/who-we-are
- s/a, *Wikileaks- News and Background*, [en línea], American Civil Liberties Union, 29 de noviembre 2010, Dirección URL: https://www.aclu.org/free-speech-national-security/wikileaks-news-and-background
- s/a, *Today's CIA*, Central Intelligence Agency, [en línea], 5 de abril de 2007, Dirección URL: https://www.cia.gov/about-cia/todays-cia
- s/a, *Wikileaks pone los secretos de la diplomacia de Estados Unidos al descubierto*, [en línea], Lavanguardia.com, 28 de noviembre 2010, Dirección URL:http://www.lavanguardia.com/internacional/20101128/54075940504/wikileaks-pone-los-secretos-de-la-diplomacia-de-estados-unidos-al-descubierto.html
- s/a, *Filtración de documentos diplomáticos de los Estados Unidos*, [en línea], Golden Map, http://es.goldenmap.com/Filtraci%C3%B3n_de_documentos_diplom%C3%A1ticos_de_los_Estados_Unidos#Censura_y_prohibici.C3.B3n_de_WikiLeaks_en_Estados_Unidos.2C_China_y_Francia
- s/a, *Definition PKI,* [en línea], Search Security, Dirección URL: http://searchsecurity.techtarget.com/definition/PKI
- s/a, *Wikileaks: las diez peores cosas que dijo EE.UU. de Cristina y del Gobierno*, [en línea], MDZ Online, 30 de noviembre 2010, http://www.mdzol.com/nota/255989/
- s/a*, Ecuador expulsa a la embajadora de EU tras un cable de WikiLeaks,* [en línea], CNN México, 5 de abril de 2011, Dirección URL:http://mexico.cnn.com/mundo/2011/04/05/ecuador-expulsa-a-la-embajadora-de-eu-tras-un-cable-de-wikileaks
- s/a, *The National Security Agency: Mision, Authorities, Oversight and Partnerships*, [en línea], FAS, 9 de agosto 2013, Dirección URL:https://www.fas.org/irp/nsa/nsa-story.pdf

- s/a, *US fumes over WikiLeaks release of diplomat memos***,** [en línea], WikiLeaks Diplomatic Disclosures, The News, 28 noviembre 2010, Dirección URL:http://www.geo.tv/important_events/2010/wikileaks/pages/english_news_28-11-2010.asp
- *s/a, Perfil Carlos Pascual, de Stanford y de Harvard a México*, [en línea], México, El Universal, 26 de marzo de 2009, Dirección URL:http://www.eluniversal.com.mx/notas/586468.html
- s/a, *Uniting and Strengthening America by providing appropriate tools required to intercept and obstruct terrorism (USA Patriot Act) Act 2001*, [en línea], 26 de octubre de 2001, Dirección URL:http://www.gpo.gov/fdsys/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf
- s/a, *La Comunidad de Inteligencia Norteaméricana,* [en línea], Intel Page, Dirección URL: http://www.intelpage.info/web/exterior/estadosunidos.htm

Anexo1 “Principios de Johannesburgo sobre Seguridad Nacional, Libertad de Expresión y acceso a la información”

1. (…) d) Ninguna restricción a la libertad de expresión o de información por razones de seguridad nacional pueden ser impuestas salvo que el gobierno pueda demostrar que la restricción esté prescripta en la ley y sea necesaria en una sociedad democrática para proteger un interés legítimo de la seguridad nacional.

1.1. (…) b) La ley debería proveer para adecuadas salvaguardas contra el abuso, incluida pronta y efectiva revisión judicial de la validez de la restricción, por una corte o juez independiente.

1.3. Para establecer que una restricción a la libertad de expresión o de información es necesaria para proteger un interés legítimo de la seguridad nacional, un gobierno debe necesariamente demostrar que:

a) esa expresión o información pone en seria amenaza a un legítimo interés de la seguridad nacional,

b) la restricción impuesta es la menos restrictiva posible para proteger ese determinado interés.

c) la restricción es compatible con principios democráticos.

2. a) Una restricción para ser justificable en el terreno de la seguridad nacional no es legítima a menos que su propósito genuino y su efecto demostrable es proteger la existencia de un país o su integridad territorial contra el uso o amenaza de la fuerza o su capacidad para responder a ellas tanto desde una fuente de agresión externa como una amenaza militar o una fuente interna tales como incitación a la expulsión violenta de un gobierno.

b) En particular, una restricción para ser justificable en el terreno de la seguridad nacional no es legítima si su propósito genuino y su efecto demostrable es proteger intereses no relativos a la seguridad nacional, incluyendo, por ejemplo, proteger al gobierno de críticas, molestias o exposición de obrar erróneo o para encubrir información respecto del funcionamiento de sus instituciones públicas o para establecer una particular ideología o para suprimir desórdenes.

12. Un Estado no puede denegar categóricamente acceso a toda la información relativa a la seguridad nacional, aunque puede designar por ley sólo aquella específica y determinada categorías de información que es necesaria retener o negar en orden a proteger un interés legítimo de la seguridad nacional.

13. En todas las leyes concernientes al derecho de obtener información, el interés público a conocer la información deberá ser la primera consideración[282].

[282] Véase: Damián Loreti y Luis Lozano, El caso Wikileaks y su relación con el derecho a la información, [en línea], Catedra, Dirección URL:http://www.catedras.fsoc.uba.ar/loreti/documentos_de_la_catedra/wikileaksdali.pdf, p 9. [Consultado el 6 de mayo de 2014].