UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE CIENCIAS POLÍTICAS Y SOCIALES

“EL ESPIONAJE ELECTRÓNICO EN LA ERA DE LA SEGURIDAD NACIONAL DE LOS ESTADOS UNIDOS: LOS GOBIERNOS DE GEORGE W. BUSH Y BARACK H. OBAMA”

TESIS

QUE PARA OPTAR POR EL GRADO DE LICENCIADA EN RELACIONES INTERNACIONALES PRESENTA

ANDREA BUSTAMANTE SALCEDO

DIRECTOR DE TESIS: MARCOS AGUSTÍN CUEVA PERUS

CIUDAD UNIVERSITARIA, CD. MX. 2018

Para Sergio, este trabajo fue posible gracias a ti. Por tomar mi mano durante el largo trayecto, escucharme, aconsejarme y creer en mí; pero sobre todo, por el amor y la felicidad. Gracias, gracias, gracias.

Para mi papá y mi mamá, gracias por su apoyo en todos los aspectos. Por amarme, enseñarme a soñar, nunca traicionar sus principios y por siempre estar del lado correcto de la historia, aún en los tiempos más adversos.

Para las mujeres en mi familia, mujeres de lucha e ideales, por mostrarme como vivir y sobrevivir.

Para mis amigas y amigos, por hacer del mundo un mejor lugar para vivir.

Para los que partieron durante este periodo de mi vida. A mi abuelita, a mi tía Arcelia y a mi tío Erasmo.

Para Layla, por su compañía en las noches de desvelo.

"All you need is love"

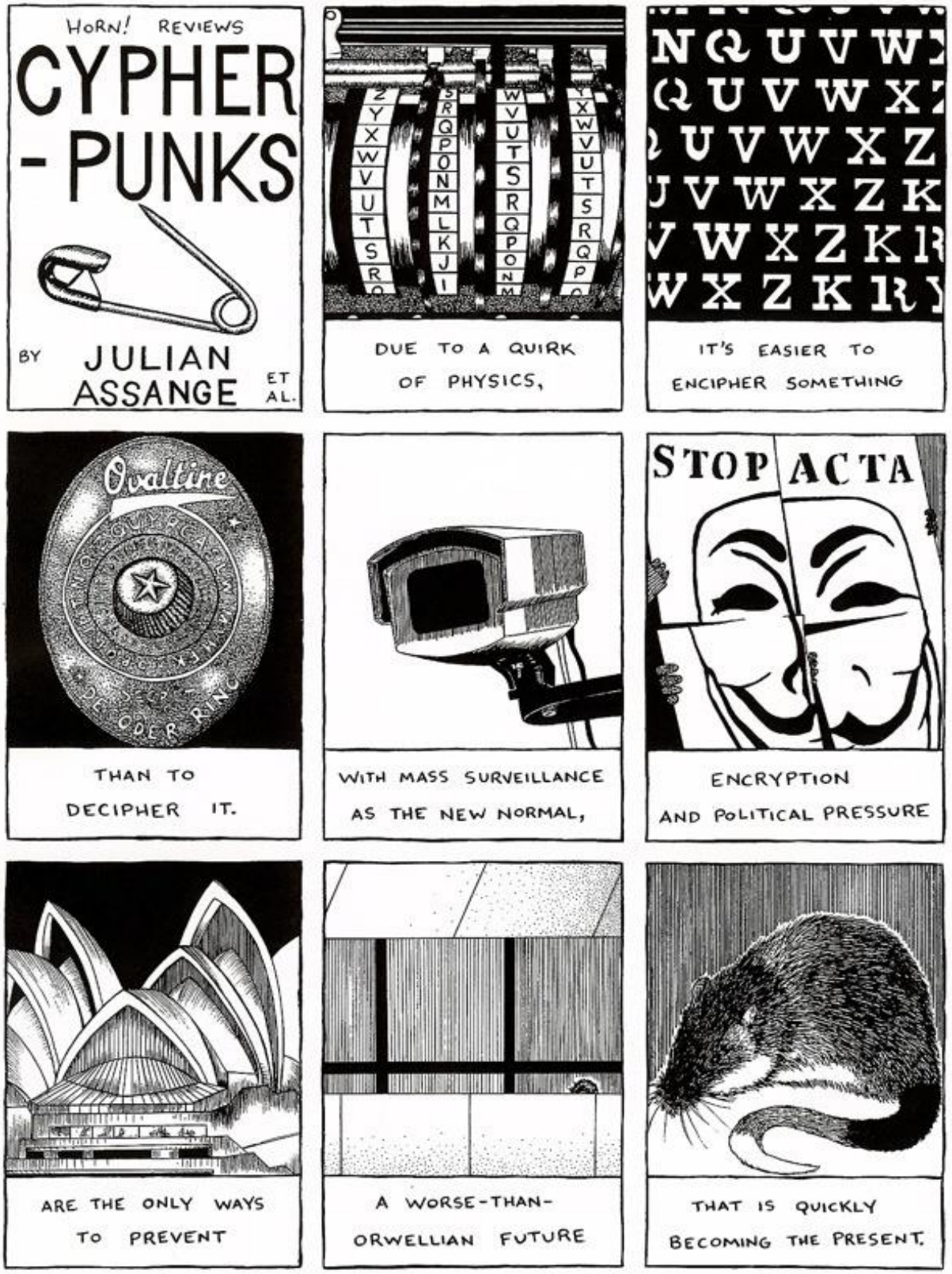
Agradecimientos

Agradezco al pueblo de México por defender a la UNAM y permitir mi formación profesional. Trabajaré para regresar lo mucho que recibí y defenderé mi alma máter para las futuras generaciones.

A la Universidad Nacional Autónoma de México y a la Facultad de Ciencias Políticas y Sociales por brindarme educación gratuita y de calidad.

Con atento agradecimiento a mi director de tesis Dr. Marcos Agustín Cueva Perus por su confianza, paciencia, consejos y por su invaluable aportación a la investigación. A mis lectores, Dra. Laura Páez Díaz de León, Dr. Héctor H. Zamitiz Gamboa, Mtro. Miguel Ángel F. Valenzuela Shelley y al Dr. Juan Manuel Contreras Colín, por su tiempo y su dedicación a la formación de los alumnos.

Ciudad de México, octubre 2018


HORN! REVIEWS
CYPHER-PUNKS
BY JULIAN ASSANGE ET AL.
DUE TO A QUIRK OF PHYSICS,
IT'S EASIER TO ENCIPHER SOMETHING
Ovaltine
THAN TO DECIPHER IT.
WITH MASS SURVEILLANCE AS THE NEW NORMAL,
STOP ACTA
ENCRYPTION AND POLITICAL PRESSURE
ARE THE ONLY WAYS TO PREVENT
A WORSE-THAN-ORWELLIAN FUTURE
THAT IS QUICKLY BECOMING THE PRESENT.

ÍNDICE

Introducción. La guerra por todos los medios

El 11 de septiembre de 2001 aturdió al mundo. Yo estudiaba la secundaria. Ese día, mi madre me pasó a recoger a la escuela como diariamente hacía. En la radio del automóvil resonó la noticia de la caída de las Torres Gemelas en la ciudad de Nueva York. En ese entonces no entendí por qué el mundo estaba de tal modo impactado.

No me refiero a que las imágenes de la caída de las torres y el choque de los aviones contra éstas no fueran motivo suficiente para impresionarme, lo que quiero decir es que, en esos momentos, no comprendí que Estados Unidos era la potencia militar más poderosa del mundo, ni tenía conocimiento de sus alcances bélicos, mucho menos de sus sistemas de espionaje.

Tampoco conocía del dolor causado a México, ni a otros pueblos, por las acciones imperialistas de ese país. En cambio, sí conocía su moda, cine, programas de televisión, música, ciudades llenas de rascacielos. Del *american dream*, luego pues. En contraste, poco sabía de cine mexicano, de música mexicana, de nuestra ropa típica, de nuestros pueblos y de nuestras ciudades. Y de América Latina, mejor ni hablar.

Poco sabía del *soft power*. Pero lo vivía.

Más allá de la vivencia personal o de la finalidad de los perpetradores de los terribles acontecimientos de ese 11S, y digo "ese" porque también subsiste la memoria del 11 de septiembre de 1973, día del derrocamiento de Salvador Allende; En todo caso, el 11 de septiembre de 2001 en Estados Unidos y el mundo sucedió algo terrible e importante porque dio pie al discurso de la guerra contra el terror y a las consecuentes invasiones a Afganistán e Iraq.

Días después de los injustificables ataques, el 14 de septiembre de 2001 el entonces presidente de Estados Unidos, George W. Bush, pronunció un discurso mediante el cual empezó a perfilarse lo que terminaría por convertirse en uno de los

argumentos ejes de la Seguridad Nacional: la guerra contra el terrorismo.

Entonces afirmó:

> A sólo tres días de estos eventos, los estadunidenses no tenemos la distancia histórica suficiente. Sin embargo, nuestra responsabilidad con la historia es clara: responder a estos ataques y librar al mundo del mal.
>
> Con sigilo, engaños y muerte han desatado la guerra contra nosotros. Esta nación es pacífica, pero feroz cuando se le aviva la rabia. Este conflicto comenzó en tiempo y términos de otros; terminará en la hora y a la manera que nosotros elijamos.[1]

El discurso se tradujo en acciones concretas: el 7 de octubre de ese mismo año, Estados Unidos y su aliado Gran Bretaña lanzaron operaciones militares en Afganistán. Libertad duradera *(Enduring freedom)* fue el nombre de la operación estadunidense. El argumento para invadir Afganistán fue que ese país albergaba al líder de la organización *Al-Qaeda*, Osama Bin Laden, autor intelectual de los atentados, e incluso permitía la libre circulación de grupos talibanes y campos de entrenamiento a los mismos. Con respecto al derecho internacional, Estados Unidos justificó la invasión a Afganistán con base en el artículo 51 del capítulo VII de la Carta de las Naciones Unidas, que dice:

> Ninguna disposición de esta Carta menoscabará el derecho inmanente de legítima defensa, individual o colectiva, en caso de ataque armado contra un miembro de las Naciones Unidas, hasta en tanto el Consejo de Seguridad haya tomado las medidas necesarias para mantener la paz y la seguridad internacional. Las medidas tomadas por los miembros en ejercicio del derecho de legítima defensa serán comunicadas inmediatamente al Consejo

[1] George W. Bush, "Remarks at the National Day of Prayer and Remembrance Service", *American Speeches, Political oratory from Patrick Henry to Barack Obama*, p. 331. [traducción propia]

de Seguridad, y no afectarán en manera alguna la autoridad y responsabilidad del Consejo conforme a la presente carta para ejercer en cualquier momento la acción que estime necesaria con el fin de mantener o restablecer la paz y la seguridad internacional.[2]

Estados Unidos invadió Afganistán con la base jurídica de la legítima defensa contra una agresión. "La Asamblea General de la ONU se ocupó del tema en la Resolución 1314 que define lo que es la agresión: 'La agresión es el uso de la fuerza armada por un Estado contra la soberanía, la integridad territorial o la independencia política de otro Estado, o en cualquier otra forma incompatible con la Carta de las Naciones Unidas […]'".[3] Sin embargo, y a pesar de que un grupo terrorista no es un Estado, "[…] el Consejo de Seguridad, frente a los atentados del 11 de septiembre se limitó a condenar el terrorismo y a reconocer el derecho de legítima defensa inmanente de Estados Unidos en las resoluciones 1368 del 12 de septiembre de 2001 y 1373 del 28 de septiembre de 2001." [4]

No se trata de entablar una discusión sobre si las resoluciones de la Organización de Naciones Unidos fueron condescendientes con Estados Unidos, o si este país ejerció presión como miembro permanente del Consejo de Seguridad para que las resoluciones fueran votadas acorde con sus intereses, motivo sin duda de serios cuestionamientos que aquí no se abordan. De lo que se trata es de situar el marco temporal en que se desarrolla el presente trabajo.

De la acción a la doctrina

Una doctrina es el "conjunto de ideas u opiniones religiosas, filosóficas, políticas,

[2] Artículo 51, "Capítulo VII: Acción en caso de amenazas a la paz, quebrantamientos de la paz o actos de agresión", *Carta de Naciones Unidas*, http://www.un.org/es/sections/un-charter/chapter-vii/index.html
[3] Octavio Augusto Caro Garzón, "La doctrina Bush en la guerra preventiva: ¿Evolución del 'ius ad bellum' o vuelta al Medievo?", *Revista FACULTAD DE DERECHO Y CIENCIAS POLÍTICAS*. Vol. 36, No. 105, Medellín-Colombia, Julio-Diciembre de 2016, p, 415.
[4] *Ibíd.*, p. 418.

etcétera sustentadas por una persona o grupo".[5] La historia de Estados Unidos, por sólo referirnos a la época posterior a la Segunda Guerra Mundial, contempla numerosas doctrinas. Por ejemplo, la doctrina Eisenhower, la doctrina Carter, la doctrina Clinton[6]. Todas éstas se tradujeron en acciones políticas y militares. Es así que: "El 26 de septiembre de 2001, el secretario adjunto de la Secretaría de Defensa de Estados Unidos, Paul Wolfowitz, manifestaba en la reunión de ministros de defensa de la [Organización del Tratado del Atlántico Norte] OTAN, que la respuesta de Estados Unidos a los atentados terroristas sería 'multidimensional, multifacética y de larga duración'".[7]

Aunque aún no estaba delineada la doctrina Bush, era evidente que las respuestas a los ataques del 11 de septiembre consistirían en acciones bélicas desde diversos ámbitos, y que no terminarían en un corto plazo. Meses después, "[…] el 29 de enero de 2002 [en *West Point*], las cosas se hicieron aún más claras. Se incluyó a Sadam Hussein, junto a Corea del Norte e Irán, en lo que el presidente Bush llamó el 'Eje del Mal' *(Axis of evil).* […] las intenciones de la administración Bush iban más allá de la desarticulación de las redes terroristas de *Al-Qaeda* que operaban en Afganistán. El objetivo ahora era más amplio, no sólo la eliminación de la amenaza terrorista que había desencadenado el 11 de septiembre, sino también la eliminación de cualquier eventual amenaza proveniente de una organización terrorista o de un régimen que probablemente tuviera armas de destrucción masiva en su poder."[8]

Pasaron muchos años, hasta llegar 2013, para que pudiésemos enterarnos que como consecuencia del 11 de septiembre de 2001, el presidente Bush impuso una serie de programas de vigilancia nacional y global, conocidos como "el programa del presidente", implantados en el marco de la guerra contra el terror. Esto se supo por una serie de documentos filtrados por el exempleado de la Agencia de Seguridad

[5] *Diccionario de la lengua española,* Real Academia Española (RAE), edición del tricentenario, actualización 2017, entrada: doctrina, http://dle.rae.es/?id=E3eOaI9
[6] Las doctrinas Eisenhower, Carter y Clinton se desarrollan en el glosario.
[7] Octavio Augusto Caro Garzón, *op. cit,* p. 419.
[8] *Ibíd.,* p. 420.

Nacional, Edward J. Snowden.

Barack H. Obama fue presidente después de George W. Bush. El primero llegó al Ejecutivo por el Partido Demócrata, mientras el segundo lo logró en representación del Republicano. No obstante, Obama continuó con los programas de vigilancia instaurados por el primero. Es decir, a pesar del cambio de partido, las estructuras de Inteligencia de Estados Unidos operaron sin modificar dichos programas. Es en este marco histórico en el que se analizan los programas de espionaje.

Como dijo el internacionalista indio Achin Vanaik: "actualmente, Estados Unidos es, con mucho, la mayor potencia militar del mundo. ¿Quién podría dudar de ello? Nadie debería extrañarse tampoco de que sus élites dirigentes busquen mantener, extender y profundizar la dominación política estadunidense. Las principales líneas que dividen a dichas élites tienen que ver con el cómo llevar a cabo esta tarea."[9]

Por tanto, cabe la pregunta: ¿Para qué espía Estados Unidos? La respuesta parece simple: Para obtener y preservar el poder en dos niveles: hacia adentro, en su sociedad; y hacia afuera, en el que ejerce en las sociedades externas. Este trabajo es un intento por demostrar que toda forma de espionaje no es sino un método de preservación de poder que se desarrolla con continuidad, por lo menos desde la segunda posguerra mundial.

Acorde con este planteamiento, lo que se pretende es analizar al sistema de Inteligencia estadunidense, poniendo mayor énfasis en la Agencia de Seguridad Nacional, por ser ésta la dependencia encargada de los programas de espionaje electrónico que se han desarrollado desde la segunda mitad del siglo XX; las implicaciones que ha tenido el espionaje en su versión convencional y ahora el ciberespionaje, para servir como herramienta de poder en consonancia con un proyecto de nación. Al final, como dijo Jeremy Bentham en su obra *Panopticon,*

[9] Achin Vanaik, (ed.), "Introducción: actualizada en noviembre de 2010", *Casus belli: cómo los Estados Unidos venden la Guerra*, Transnational Institute at Smashwords, 2011, e-book, p. 11.

vigilar es "un 'medio de obtener el poder, un poder sobre la mente […]".[10] Las nuevas tecnologías facilitan la tarea.

Mucha de la información que se obtuvo para el desarrollo de esta tesis se debe a las filtraciones de valientes ciudadanos del mundo, algunas veces miembros de la rama militar o de la comunidad de Inteligencia, que decidieron obedecer a una moral interior, incluso si ponían en riesgo su libertad, y filtrar la información aun a costa de la ruptura de mando, que en esos círculos es tan importante.

De tal manera, esta investigación pretende reflexionar acerca de la vigilancia en las sociedades modernas y su relación con el poder. En específico, el presente estudio se centra, dentro de este gran tema, en los mecanismos que el gobierno estadunidense ha utilizado para espiar (tanto a otros países como a su propia sociedad) y en su constante sofisticación.

Dicha sofisticación ha provocado severos cuestionamientos entre los propios encargados de ejercer la vigilancia sobre cuáles deberían ser sus límites, en un contexto en que de manera paralela, el debate acerca de los contornos que definen los derechos humanos sigue abierto y la tensión vigilancia *versus* libertad parece aumentar.

Marco teórico

En un primer momento parecería que los programas de espionaje que se revelaron a partir de junio de 2013 son consecuencia directa de su contexto histórico inmediato, y en cierto sentido lo son. Sin embargo, como se verá a lo largo del desarrollo de los capítulos, no son los primeros programas de espionaje que existen, ni los primeros que despliega Estados Unidos en el ámbito global. Por ejemplo, el tratado UKUSA funciona desde el término de la Segunda Guerra Mundial.

El problema estriba en que los programas de espionaje actuales se desarrollan en el marco de las tecnologías de la información y la comunicación.[11] Nunca antes

[10] Armand Mattelart, Gilles Multigner (trad.), *Un mundo vigilado*, Barcelona, Paidós, 2009, p. 17.
[11] Tecnologías de la información y las comunicaciones. Engloban medios de comunicación y las aplicaciones

habían tenido este alcance porque la tecnología tampoco había evolucionado a su estado actual. La tecnología, entonces, se presenta como herramienta determinante para el sistema de Inteligencia, lo que le brinda a éste un inmenso poder.

No es la intención de este análisis utilizar neologismos técnico comunicacionales, sin embargo, es irremediable, pues detrás de los conceptos existe una carga ideológica que promueve el desarrollo de cierta ciencia y cierta tecnología. Dicho de una manera más precisa por el sociólogo belga Armand Mattelart: "Las creencias de las que la noción de sociedad de la información es portadora desencadenan fuerzas simbólicas que impulsan a actuar, a la vez que permiten actuar, en un determinado sentido y no en otro. Orientan la formulación de programas de acción y de investigación por parte de los Estados y de los organismos supranacionales."[12]

El punto de partida de esta fuerza tecnológica que se fusiona con el aparato militar-industrial está marcado por el decisivo desempeño que tuvo la tecnología belicista en la Segunda Guerra Mundial. "En 1947, el modelo de sinergia experimentado contra las potencias del Eje por científicos, sector privado y necesidades de la defensa es conducido por la *National Security Act* [Ley de Seguridad Nacional, la cual se puntualiza en el primer capítulo]. Esta vez, con el propósito de unir a los actores de la innovación técnica contra el enemigo catalogado como global: el comunismo mundial".[13]

Es en ese mismo año cuando surge el Pentágono como aparato de cohesión de las tres ramas militares de Estados Unidos: terrestre, marina y aérea. "El Pentágono, […también tiene] a su cargo el otro gran objetivo de la Ley de Seguridad Nacional: continuar con las sinergias en materia de investigación y desarrollo entre militares e

---

de información. Son el conjunto de medios de comunicación y las aplicaciones de información que permiten la captura, producción, almacenamiento, tratamiento y presentación de informaciones. Entrada: Tecnologías de la información y las comunicaciones, *EcuRed*, https://www.ecured.cu/Tecnologías_de_la_información_y_las_comunicaciones

[12] Armand Mattelart, Gilles Multigner (trad.), *Historia de la sociedad de la información*, Barcelona, Paidós, 2002, p. 12.

[13] *Ibíd.*, p. 56.

investigadores de los ramos civiles, industrial y universitario."[14]

Por tales razones, cuando en este trabajo se hace referencia al imperialismo, pese a que existen múltiples teorías para explicarlo, se acude a la interpretación de los economistas estadunidenses neomarxistas: Paul Baran y Paul Sweezy. De una manera sencilla, el imperialismo puede explicarse como aquella política estatal que busca el dominio de otro Estado o la subordinación de éste a intereses políticos, económicos y/o militares. Sin embargo, la contribución de estos autores al concepto de imperialismo radica en que:

> Estados Unidos no habría podido tener en la última posguerra un desarrollo económico tan rápido y de dimensiones tan impresionantes si no hubiera empleado gran parte de su presupuesto en armamentos. Dichos gastos permiten tener ocupada en servicios militares directos e indirectos (sectores productivos que trabajan para la defensa) a gran parte de la población que de otro modo sería improductiva. Además, los gastos militares son un instrumento bastante efectivo para favorecer el desarrollo tecnológico, ya que gran parte de las invenciones más importantes, usadas después en el sector civil, proceden de la actividad de investigación del sector militar.[15]

Ya en el marco de la Guerra Fría, "en 1958, año crucial si los hay, ya que el año anterior la Unión Soviética había desafiado a Estados Unidos con el lanzamiento del satélite Sputnik, abriendo así un nuevo frente en la Guerra Fría: la lucha por la conquista del espacio, el Pentágono crea una nueva agencia de coordinación de los contratos federales de investigación, la *Defense Advanced Research Projects Agency* (DARPA). Diez años más tarde, con el fin de facilitar los intercambios entre los distintos equipos contratantes, esta agencia inaugura la red Arpanet, antepasado de

[14] Armand Mattelart, Gilles Multigner (trad.), *Un mundo vigilado*, *op. cit.,* p.73.
[15] Entrada: Imperialismo, Sergio Pistone en Norberto Bobbio, Nicola Matteucci y Gianfranco Pasquino (bajo la dirección de) Raúl Crisafo, et. al. (trad.), *Diccionario de política*, Edo. de México, Siglo XXI, 2008, volumen I de la a a la j, p. 790.

internet."[16]

La información en el siglo XXI

El sociólogo Manuel Castells, en su libro *Comunicación y poder* nos advierte que "el poder se basa en el control de la comunicación y la información, ya sea el macropoder del Estado y de los grupos de comunicación, o el micropoder de todo tipo de organizaciones".[17]

El espionaje del siglo XXI, en consecuencia, tendría como finalidad obtener la información de los enemigos en la red y desde la red a partir del uso de tecnología. Dada la concentración de capital tecnológico en el mundo, Estados Unidos tiene la potencia para vigilar y almacenar una inmensa cantidad de información. Esto, a través de la comunidad de Inteligencia y el complejo tecnológico en California conocido como *Silicon Valley.* "De igual manera que con los conductos petroleros sucede con los cables de fibra óptica. El control físico de los flujos gigantes de información que conectan a la civilización global […] es un nuevo juego: controlar la comunicación de billones de personas y organizaciones".[18]

El debate surgió en todo el mundo, sin embargo, se centró en Estados Unidos, se enfocó en los datos o data, en quién posee la mayor capacidad tecnológica para almacenar los miles de millones de datos que existen en la web y qué hacer con ellos.

Es decir: la información es poder.

La retórica

La Seguridad Nacional es "el 'lenguaje propio de todo lo que se refiere al Imperio', añade Joseph Comblin en su historia de la ideología de la Seguridad Nacional […] [Es] un 'símbolo' cargado con todos los 'valores místicos del Imperio mismo'.

[16]Armand Mattelart, Gilles Multigner (trad.), *Historia de la sociedad de la información*, *op. cit.,* p. 62.
[17]Manuel Castells, María Hernández (trad.), *Comunicación y poder*, Madrid, Alianza Editorial, 2009, p. 23.
[18]Julian Assange, María Maestro *(trad.), Cypherpunks. La libertad y el futuro de Internet*, México, D.F., Planeta Mexicana, 2013. p. 13.

Porque la Seguridad Nacional consiste en 'ese valor del que siempre se está hablando y que no necesita ser explicado ni justificado […]"[19].

Además, la retórica está dotada de carácter moral y religioso: "[…] para el historiador [británico] David Reynolds, quien poco después de la caída del Muro de Berlín escribe un estudio sobre los orígenes de la Guerra Fría, la Seguridad Nacional ha de leerse como un 'evangelio' que reactiva el proyecto mesiánico formulado por el presidente Wilson hacia el final de la Gran Guerra, de remodelación del orden mundial, en el que Estados Unidos 'puede y debe utilizar su poder para exportar los valores liberales, capitalistas, democráticos y anticoloniales'".[20]

El discurso de la Seguridad Nacional también justifica el uso de las nuevas tecnologías en los aparatos de Inteligencia y en la vigilancia masiva. Los antecedentes de las actuales tecnologías y el uso militar del concepto de Seguridad Nacional surgen en el mismo momento. Al respecto, Armand Mattelart y André Vitalis argumentan que: "[…] lo que comienza en la posguerra es la Guerra Fría y la creación de un contexto marcado por la bipolarización. Los dictados de la Seguridad Nacional se inscriben en tensión con las libertades individuales. El Estado americano pone los fundamentos de un complejo militar-industrial, en cuyo seno se inventan los grandes sistemas teleinformáticos que servirán de matriz al conjunto de futuros dispositivos de vigilancia masiva".[21]

Es así que surgieron nuevos conceptos: guerra cibernética, ciberofensiva, armas cibernéticas, redes sociales, centros de datos, etcétera.[22] La seguridad cibernética aparece en la "Estrategia de Seguridad Nacional, [de] septiembre de 2002", como una de las vulnerabilidades para la Seguridad Nacional. Esto responde a una época tecnológica concreta en la que las tecnologías de la información y la comunicación son determinantes para la vida de un país como el estadunidense. Esto se encuentra íntimamente relacionado con la legítima defensa y la guerra

[19] Armand Mattelart, *Un mundo vigilado, op. cit.,* p. 67.
[20] *Ídem.*
[21] Armand Mattelart, André Vitalis, Juan Carlos Miguel de Bustos (trad.), *De Orwell al cibercontrol*, Barcelona, Gedisa, 2015, p. 17.
[22] Véase glosario de términos.

preventiva.[23] Al respecto, debemos tener en cuenta lo siguiente:

> Si durante la Guerra Fría […] justificaban el comportamiento de Estados Unidos en materia de política exterior como una 'postura defensiva' necesaria para 'contener' la amenaza del comunismo y de la URSS, hoy el carácter descaradamente ofensivo de la política exterior estadunidense ya no se puede disfrazar y, por lo tanto, necesita más que nunca de discursos legitimadores. […] Al parecer, un posible discurso general –el de la 'expansión de la libertad' a través del imperialismo– no acaba de reunir todas las condiciones indispensables. Por tanto, se ha echado mano de toda una serie de discursos legitimadores, en cierta medida porque el dominio mundial no sólo exige un único discurso, sino discursos separados y matizados que permitan justificar las acciones de Estados Unidos en distintas partes del mundo con contextos políticos diversos; es decir, donde existan diversos argumentos y lógicas que expliquen la presencia estadunidense.[24]

Las tecnologías de la información son un espacio e incluso un dominio en disputa, son una fuente de poder que Estados Unidos utiliza para recopilar información a través de la vigilancia. Empero, la magnitud de aquéllas es tal que necesitan de la industria privada en este rubro para controlar el flujo de información. Aquí es donde se unen política, milicia y economía en nombre de la democracia de la información y la lucha contra el terrorismo. "En lugar de la gran bandera ideológica de la era de la Guerra Fría –la defensa del 'mundo libre' frente a la amenaza comunista– han surgido seis banderas ideológicas; todas ellas, en mayor o menor medida, al servicio de los intereses de construcción imperial estadunidenses. Estas seis banderas serían:

[23] Guerra preventiva, ver glosario.
[24] Achin Vanaik, "Introducción: actualizada en noviembre de 2010", *Casus belli: cómo los Estados Unidos venden la Guerra*, *op. cit.,* pp. 11 y 12.

(1) la guerra global contra el terrorismo (GGT),

(2) las armas de destrucción en masa (ADM),

(3) los Estados fallidos,

(4) la necesidad y la justicia de intervenciones humanitarias externas y forzosas,

(5) el cambio de régimen en nombre de la democracia, y

(6) la guerra contra las drogas."[25]

Este trabajo es un ejercicio descriptivo que, a través del análisis de los programas de espionaje a partir del fin de la Segunda Guerra Mundial, el marco jurídico, las actuales trasnacionales de la tecnología de la comunicación y el avance tecnológico, nos acercan al concepto de Armand Mattelart: Matriz tecnomilitar.

Esto quiere decir que el desarrollo científico-tecnológico tiene detrás al aparato industrial-militar que se justifica con el concepto de Seguridad Nacional y se consolida con la Comunidad de Inteligencia. Cabe entonces preguntarnos: "¿Cómo se han implantado unos sistemas sociotécnicos que han ampliado el área de competencia de las tecnologías inquisitoriales de las libertades individuales y colectivas y que son tributarios de su genealogía policial o militar?".[26]

Estructura de la investigación

La tesis está dividida en tres capítulos que se inscriben así:

1. Arquitectura del espionaje estadunidense. Breve revisión desde la segunda mitad del siglo XX hasta los mecanismos implementados a consecuencia del 11S.

2. Ciberguerra estadunidense y *Silicon Valley*.

[25] *Ibíd.,* p. 13.

[26] Armand Mattelart, *Un mundo vigilado, op. cit.,* p.12.

3. Resistencias frente a la distopía.

La estructura del espionaje estadunidense es vasta y forma parte del aparato estatal. Incluso cuenta con la Oficina del Director de Inteligencia, misma que integra a las diversas agencias, las cuales atraviesan toda la estructura gubernamental y en conjunto conforman a la Comunidad de Inteligencia.

Este aparato multiagencia no es circunstancial al gobierno, es intrínseco a un proyecto de Estado-nación. Por esta razón encuentra su lógica y justificación en el concepto de Seguridad Nacional. Al aclarar este punto, mediante un análisis del espionaje en su fase actual, podemos realizar una aproximación al papel de la vigilancia en el proyecto de nación de Estados Unidos.

Pero antes debemos comprender el alcance de un aparato de Inteligencia sustentado en un amplio arsenal normativo. Con tal propósito se analizarán algunas de las leyes condensadas en la publicación del Departamento de la Defensa *Intelligence Community Legal Reference Book.* Bajo este conjunto de leyes, se enmarcan los programas de espionaje que se analizan en el primer capítulo.

En este tenor, no es casual que exista una red de vigilancia supraestatal de las comunicaciones, cuyo funcionamiento también se aborda en el primer capítulo, la cual incluye a cinco países: Estados Unidos, Gran Bretaña, Australia, Nueva Zelanda y Canadá, misma que surge como resultado de la Segunda Guerra Mundial y que funciona hasta nuestros días.

Todo esto servirá como preludio para entrar en la materia específica del tema a desarrollar: las dimensiones del espionaje estadunidense en la era tecnológica actual. Me tomo la libertad de decir que el primer capítulo es la introducción o aproximación al tema, además de identificar su contexto e historicidad.

En el segundo capítulo: Ciberguerra estadunidense y *Silicon Valley* se examinan, para empezar, tres Estrategias de Seguridad Nacional, las de 2002, 2010 y 2015. La primera se enmarca en el periodo presidencial de George W. Bush. Y las

dos últimas en el de Barack H. Obama. En ellas se hace uso, por primera vez, del concepto de seguridad cibernética en una Estrategia de Seguridad Nacional.

Este apartado surge como documentación probatoria del interés que tiene el gobierno de Estados Unidos por el ámbito cibernético. Espacio que es considerado el quinto dominio después del mar, la tierra, el agua, el aire y el espacio. Existe una nueva nomenclatura en torno de este lugar de disputa que abarca desde seguridad cibernética hasta las operaciones ofensivas y defensivas y la superioridad en el espacio cibernético.

Estados Unidos, además de la conceptualización de guerra que ha hecho de este espacio, cuenta con armamento para crear una ventaja tecnológica-bélica de dimensiones inimaginables, lo que no debería de sorprendernos. Porque el espacio cibernético, entendido como las redes computacionales conectadas y no conectadas a internet, es de gran utilidad para los Estados. La digitalización de la información podría considerarse una de las características de las sociedades actuales.

Después de analizar el arsenal cibernético y algunas armas que conciernen a este lugar, se desarrolla *Silicon Valley* y su relación con el gobierno estadunidense, así como el alcance mundial de empresas como AT&T, Verizon, Level 3, Google y Facebook.

El tercer y último capítulo comienza con una descripción de la criptografía. Frente a la vigilancia con las capacidades tecnológicas actuales, el uso de la criptografía resultó uno de sus más fieros combatientes. Como nos daremos cuenta, la criptografía o los mensajes encriptados han sido utilizados desde los romanos hasta llegar a los criptopunks y criptoanarquistas.

En la segunda parte de este capítulo, denominado "Arquitectura de la opresión", se abordan filtraciones que cambiaron la manera de entender a los servicios de Inteligencia. Se abarca desde Duncan Campbell, periodista que reporta el fenómeno UKUSA, hasta las filtraciones de los *Pentagon Papers*, *WikiLeaks* y los documentos Snowden, así como la respuesta del gobierno estadunidense a cada una

de ellas. La vigilancia masiva es muy poderosa. Pero también lo ha sido la lucha contra ella.

Aclaración

Esta tesis contiene imágenes de documentos oficiales cuyo objetivo es sustentar lo expuesto de la mejor manera posible. El tema no es sencillo y puede prestarse a malinterpretaciones. Indagar en las entrañas de los aparatos de Inteligencia exige, como cualquier investigación, una ardua dedicación, pero además es un tema en el que el investigador muchas veces parece quedarse sin piso firme en dónde sostenerse.

Por tal razón, se muestran algunos de los documentos investigados, en particular aquellos que corresponden a filtraciones. Cabe aclarar que una filtración no debe de entenderse como una invención. Una filtración es un documento compartido a la opinión pública por una persona o grupo de personas que deciden que sería mejor para una sociedad que fuese de dominio público. De otra forma la información existiría, pero sólo sería de conocimiento restringido.

1

Arquitectura del espionaje estadunidense. Revisión desde la segunda mitad del siglo XX hasta los mecanismos implementados después del 11 de septiembre de 2001

> "No había rincón del mundo en el que no hubiera un supuesto interés en peligro o bajo ataque real. Si los intereses en riesgo no eran romanos, eran de los aliados de Roma; y si Roma no tenía aliados, entonces se inventaba algunos. Cuando era imposible inventar tal interés, entonces por casualidad era el honor nacional el que había sido insultado…Roma siempre estaba siendo atacada por malvados vecinos."
>
> (Joseph Schumpeter)[27]

El espionaje es realizado por las agencias de Inteligencia , mismas que en lo subsiguiente serán llamadas así, agencias de Inteligencia o agencias de espionaje, porque la literatura especializada tiende a hacer uso indistinto de ambos términos. Las agencias de Inteligencia /espionaje se dedican a esta primera actividad, la Inteligencia, gracias a los insumos que brinda la segunda, el espionaje. Empero, no son sinónimos. Desglosemos ambos conceptos.

En su libro *Guerra en la red. Los nuevos campos de batalla*, Richard A. Clarke, quien trabajó treinta años en el gobierno de Estados Unidos: Casa Blanca, Departamento de Estado y en el Pentágono o Departamento de Defensa,[28] define al espionaje como "las actividades de Inteligencia destinadas a recabar información, a la que otra nación (u otro actor) intenta impedir el acceso".[29]

---

[27] Joseph Schumpeter, citado por Morris Berman, Eduardo Rabasa (trad.), *Edad oscura americana. La fase final del imperio*, Madrid, Sexto Piso, 2008, p.161.

[28] El Pentágono está conformado por las oficinas centrales del Departamento de Defensa, localizadas en Arlington, Virginia. Sin embargo, son términos metonímicos. En el uso común, se utiliza el Pentágono para referirse al Departamento de Defensa, y no necesariamente al complejo arquitectónico construido con base en la figura geométrica de cinco lados que sirve como oficina administrativa para esta dependencia estatal.

[29] Richard A. Clarke, Robert K. Knake, Luis Alfonso Noriega (trad.), *Guerra en la red. Los nuevos campos de batalla*, Barcelona, Ariel, 2011, p. 362.

Para definir Inteligencia, la última versión del *Diccionario de términos militares y relacionados del Departamento de la Defensa*[30] *(Dod Dictionary of Military and Associated Terms)*, publicado en agosto de 2017, contiene tres niveles explicativos:

"1. El producto que resulta de recolectar, procesar, integrar, evaluar, analizar e interpretar información disponible, concerniente a naciones extranjeras, elementos o fuerzas hostiles o potencialmente hostiles, o áreas de operaciones actuales o potenciales. 2. Las actividades que resulten de dicho producto. 3. Las organizaciones que realizan estas actividades."[31]

Se entiende que si tuviésemos que consolidar jerarquías analíticas, la Inteligencia se encontraría por encima del espionaje. La Inteligencia es el espionaje más otras actividades, acciones y organizaciones. En cambio, el espionaje tiene una relación directa con la obtención de información primaria, sin análisis. El fin primero y último del espionaje es la obtención de información por diversos métodos, por ejemplo: la disuasión, la presión, el chantaje, las amenazas, la tortura o la vigilancia. Es ésta última, principalmente, la que atravesará por completo el presente estudio. "Por principio, toda vigilancia es exterior. Se trata siempre de seguir al individuo [o grupo de individuos], de conocer sus actividades y sus movimientos, sus contactos, y luego penetrar sus intenciones"[32].

Todos los métodos tienen una o múltiples técnicas, las cuales son el conjunto de conocimientos científicos y tecnológicos aplicados para un fin. Un ejemplo:

> Los agentes de influencia han existido siempre. Los ejemplos históricos son demasiado numerosos para citarlos todos. Generalmente se atribuye la creación de los agentes de influencia al imperio Mongol del siglo XII, según los trabajos del historiador Michael Pravdin *(The Mongol Empire)*. Lo novedoso de la técnica de la [Agencia Central de Inteligencia] CIA [por sus siglas en inglés] es, ante todo, la utilización de la ciencia y, en particular, de las matemáticas. Las teorías del sabio norteamericano Festinger sobre la dinámica de los grupos ha sido desarrollada por la Rand Corporation, la Mitre

[30] *El Diccionario de términos militares y relacionados del Departamento de Defensa* se utiliza para homologar conceptos en todas las áreas del Departamento de Defensa. Como el mismo diccionario advierte, en el prefacio de la versión de agosto de 2017, "[…] es la fuente primaria de terminología para preparar correspondencia, políticas, estrategia, doctrina y documentos de planeación".

[31] Entrada: Intelligence**,** *Dod Dictionary of Military and Associated Terms, as of August 2017*, p. 114. [traducción propia]

[32] Victor Serge, Daniel Molina (trad.), *Lo que todo revolucionario debe saber sobre la represión* [Serie popular Era/16], México, D.F., Era, 1972, p. 15.

Corporation, etc., hasta convertirlas en un arma. En adelante, la guerra psicológica ya no es un arte, sino una técnica.[33]

En este capítulo se analizan tres pilares del espionaje: la estructura de la Comunidad de Inteligencia, el marco de leyes de la misma y los programas de espionaje de las tecnologías de la información.

1.1 La Comunidad de Inteligencia

En el sitio oficial en internet de la Oficina del Director de Inteligencia Nacional (*Office of The Director of National Intelligence,* ODNI), se dice que su misión es: encabezar la integración de las agencias de espionaje y forjar una Comunidad de Inteligencia que obtenga la información más perspicaz posible.[34] La ODNI es la encargada de sistematizar la información de la Comunidad de Inteligencia *(Intelligence Community, IC).*

La Federación de Científicos Estadunidenses, FAS[35], por sus siglas en inglés, advierte en su "Reseña histórica de la evolución de la Comunidad de Inteligencia", que el espionaje ha sido una actividad del gobierno desde que se fundó Estados Unidos. La FAS hace énfasis en el papel crucial que dicho espionaje ha jugado en la asistencia a las fuerzas militares, dio forma a la política exterior y persistió durante los diferentes gobiernos. En este contexto resulta interesante notar que "[…] gran parte de lo que hoy se conoce como la Comunidad de Inteligencia fue creada y desarrollada durante el periodo de la Guerra Fría."[3637]

La FAS precisa que "con la expansión e intensificación de la Guerra Fría en las décadas de 1950 y 1960, vino aparejado el crecimiento en el tamaño y número de responsabilidades de

---

[33] Gregorio Selser, CIA: Agencia Central de Inteligencia de los Estados Unidos 1958, Fondo A, año de publicación 1958, Clave del expediente W US5, recortes y páginas de diarios, páginas de revistas y cables, CAMENA, UACM, pp. 15 y 16.

[34] "Mission, vision & goals", *Office of the Director of National Intelligence*, https://www.dni.gov/index.php/who-we-are/mission-vision

[35] La Federación de Científicos Estadunidenses fue fundada por muchos de los científicos que pertenecieron al proyecto Manhattan (ver glosario). "La FAS provee análisis y soluciones con base científica contra las amenazas de Seguridad Nacional e internacional. En específico, trabaja para reducir la proliferación de armas nucleares, prevenir el terrorismo nuclear y radiológico, promover altos estándares en seguridad de la energía nuclear, sacar a la luz prácticas gubernamentales de secretismo, así como prevenir el uso de armas químicas y biológicas" en fas.org/about-fas

[36] Guerra Fría, ver glosario.

[37] s/a, "The evolution of de U.S. Intelligence Community-An Historical Overview", Federation of American Scientists, http://fas.org/irp/offdocs/int022.html#fnt7 [traducción propia]

las agencias de espionaje para hacer frente a sus desafíos."[38] Es importante considerar qué se pensaba en esa época para comprender en qué sentido fueron en aumento el tamaño y las acciones o responsabilidades de las agencias de Inteligencia. El geopolítico y asesor del gobierno, Zbigniew Brzezinski, expresó que a principios de la década de 1960 "la era global no está ante nosotros. Ya estamos en ella. John F. Kennedy ha sido el primer presidente global porque consideraba que el mundo era, en un sentido, un problema de política interior. Esto escribe […] en *Entre dos edades. El papel de Norteamérica en la era tecnotrónica.*"[39]

1.1.1 CIA y NSA

La Comunidad de Inteligencia se forma por "todos los departamentos o agencias de un gobierno involucrados en actividades de Inteligencia. Bien en un rol de vigilancia, bien en gestión o con participación directa […]"[40]. Aunque en la actualidad son diecisiete las agencias que la forman, no siempre fue así.

El origen de la IC se encuentra al término de la Segunda Guerra Mundial. "Bendell Smith creó la Agencia Central de Inteligencia en 1947. [Allen] Dulles se unió a ella, y en 1952 fue nombrado su director general".[41] "[…] Dulles […] hermano del secretario de Estado, John Foster Dulles, […] no es nuevo en el espionaje. Durante la guerra fue uno de los altos oficiales de la Oficina de Servicios Estratégicos [OSS, por sus siglas en inglés]."[42]

La OSS fue la primera agencia central de Inteligencia y espionaje de Estados Unidos. Se le considera la antecesora de la CIA y ambas mantienen rasgos en común. Por ejemplo: "La respuesta de la OSS al desafío de preparar los operativos para las misiones tierra adentro de territorios controlados por el enemigo comenzó en 1942 con un entrenamiento paramilitar que tuvo lugar en dos parques nacionales. Uno de sus legados es el programa de entrenamiento actual de la CIA".[43]

---

[38] *Ídem.*
[39] Armand Mattelart, *Historia de la sociedad de la información*, *op. cit.,* p. 98.
[40] Entrada: Intelligence community, *Dod Dictionary of Military and Associated Terms, as of August 2017*, p. 114. [traducción propia]
[41] Gregorio Selser, CIA: Agencia Central de Inteligencia de los Estados Unidos. 1953, Fondo A, Año de publicación 1953, Clave del expediente W US3, Recortes y páginas de diarios, páginas de revistas y cables, CAMENA, UACM.
[42] Gregorio Selser, CIA: Agencia Central de Inteligencia de los Estados Unidos. 1956, Fondo A, año de publicación 1956, Clave del expediente W US4, Recortes y páginas de diarios, páginas de revistas y cables, CAMENA, UACM.
[43] Dr. John Whiteclay Chambers II, "Office of Strategic Services Training During World War II", Training for War and Espionage", *Studies in Intelligence, Vol. 54, No. 2 (June 2010)*, https://www.cia.gov/library/center-for-the-study-of-

La CIA se fundó en septiembre de 1947. Casi diez años después, en 1956, la opinión que se tenía en los medios se puede resumir con la siguiente declaración: "Como bien ha dicho un comentarista de Washington: En diez años más la Agencia Central de Inteligencia habrá igualado al servicio británico de espionaje. Por ahora su labor es útil al país, en unos años más será indispensable. Después de todo hay que recordar que estamos en una Guerra Fría y los únicos soldados que están combatiendo son los que dirige Allen Dulles".[44] Para 1958, ya eran nueve las agencias que conformaban a la Comunidad de Inteligencia.

> […] aparte de la CIA, existen ocho organismos norteamericanos que se ocupan del espionaje. Son éstos: *la National Security Agency*, la *Defense Intelligence Agency*, la *Atomic Energy Commission*, la *State Department Intelligence and Research*, la *Air Force Intelligence*, la *Army Intelligence*, la *Naval Intelligence* y la *Federal Bureau of Investigation*[45]. Estas ocho agencias tienen, ciertamente, también sus organizaciones en el extranjero […].[46]

Una demostración de cómo funcionó la Comunidad de Inteligencia en esos años fue la creación de grupos de acción secretos. En 1960 John F. Kennedy, quien fungió como presidente de Estados Unidos a partir de enero de 1961 hasta su asesinato, el 22 de noviembre de 1963, "le había encargado a Bill Harvey, un oficial superior de la Agencia Central de Inteligencia, que creara células clandestinas, las *second-story men*[47]. Éstos eran hombres que penetraban ilegalmente en las embajadas extranjeras para sustraer libros de código destinados al cifrado de las telecomunicaciones y luego las entregaban a la [Agencia de Seguridad Nacional] NSA."[48] Podemos asumir que en estas células clandestinas intervinieron agentes de la CIA y de la NSA para el análisis de la información sustraída de las embajadas.

---

intelligence/csi-publications/csi-studies/studies/vol.-54-no.-2/pdfs-vol.-54-no.-2/Chambers-OSS%20Training%20in%20WWII-with%20notes-web-19Jun.pdf , [traducción propia]

[44] Gregorio Selser, CIA: Agencia Central de Inteligencia de los Estados Unidos. 1956, Fondo A, Año de publicación 1956, Clave del expediente W US4, Recortes y páginas de diarios, páginas de revistas y cables, CAMENA, UACM.

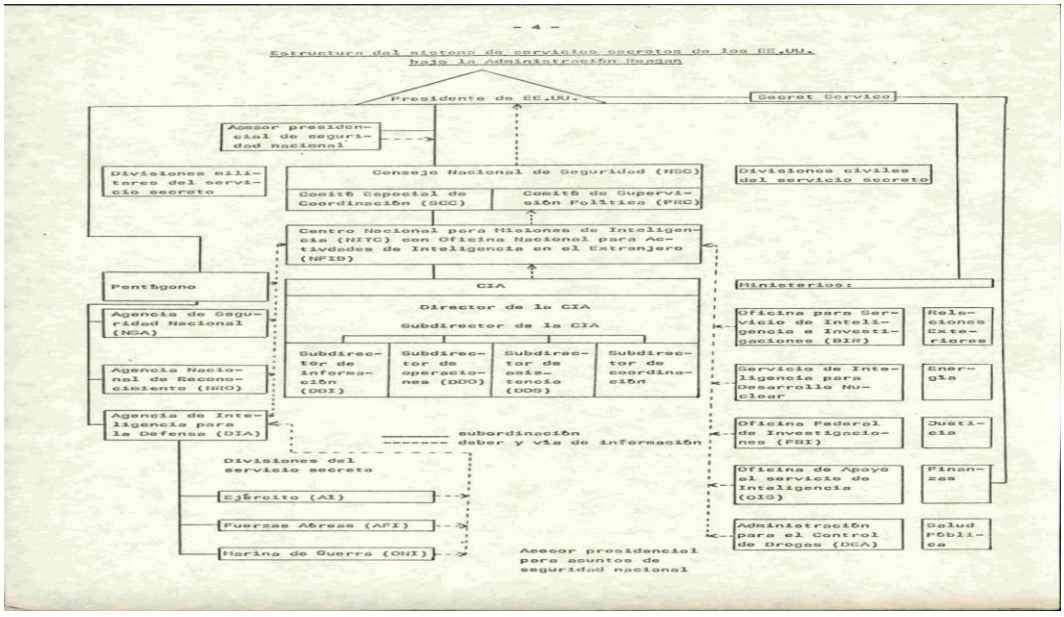
[45] En inglés, en el texto original.

[46] Gregorio Selser, CIA: Agencia Central de Inteligencia de los Estados Unidos. 1958, Fondo A, Año de publicación 1958, Clave del expediente W US5, recortes y páginas de diarios, páginas de revistas y cables, CAMENA, UACM, p. 5/18.

[47] En inglés en el texto original.

[48] Antoine Lefébure, Bárbara Poey Sowerby (trad.), *El caso Snowden. Así espía Estados Unidos al mundo,* Le Monde diplomatique, "el Dipló" y Capital Intelectual, Buenos Aires, 2014, p. 124.

En la imagen colocada debajo, hay un esquema demostrativo de cómo se estructuró la Comunidad de Inteligencia durante el gobierno de Ronald Reagan. Fue el presidente número cuarenta de Estados Unidos cuyo mandato duró dos periodos, gobernó de 1981 a 1989.[49] Según la página oficial de la Casa Blanca, el gobierno de Ronald Reagan "vio una restauración de la prosperidad en casa, con la meta de lograr la paz con el fortalecimiento en el extranjero"[50]. Para la década de los ochenta del siglo XX, ya se había ensanchado el número de agencias de Inteligencia hasta llegar a doce.



Fuente: "Estructura del servicio de los servicios secretos de EU bajo la administración Reagan", Archivo Gregorio Selser, Fondo A, CAMENA, UACM.

Hoy por hoy, la principal agencia que realiza la mayor recolección de información es la NSA. Esto se debe a que se encarga de la vigilancia a partir de tecnología electrónica. Más adelante, veremos sus alcances. La *National Security Agency* "forma parte del Departamento de Defensa. […] tiene su cuartel general en Fort Meade, Maryland, al que con frecuencia se llama sencillamente 'El Fuerte'".[51]

A la NSA se le considera una Agencia de Apoyo al Combate *(Combat Support Agency, CSA)*. Tanto la CIA como la NSA, por lo menos formalmente, están subordinadas al presidente

[49] "40. Ronald Reagan", www.whitehouse.gov/1600/presidents/ronaldreagan
[50] *Ídem.* [traducción propia]
[51] Richard A. Clarke, Robert K. Knake, *Guerra en la red. Los nuevos campos de batalla, op. cit.,* p. 365.

de Estados Unidos. La diferencia es que la CIA se encuentra en las divisiones civiles del servicio secreto; la NSA, desde su fundación respondió a las divisiones militares del servicio secreto. Sin embargo, con el paso del tiempo se diluyeron las divisiones entre los servicios secretos civiles y los servicios secretos militares. Dicho de otra manera, se militarizó a las divisiones civiles encargadas de la Inteligencia.

En el artículo de periódico intitulado "Revelación del Comité Senatorial que Investiga el Espionaje: Durante 23 Años, la ANS Interceptó las Comunicaciones de Miles de Ciudadanos Estadunidenses con el Exterior", con fecha escrita a mano del 11 de mayo de 1976, y con fuente de las agencias de medios *(Agence France-Presse*) AFP y Agencia EFE, se relata cómo "un comité del Senado puso hoy otra vez en apuros a los servicios de espionaje estadunidenses, al revelar que la Agencia Nacional de Seguridad (ANS) interceptó durante 23 años las comunicaciones de miles de ciudadanos con el exterior".[52]

Continúa:

- "La operación estaba destinada a controlar 'los contactos en el extranjero de grupos de negros, disidentes de Vietnam y otras organizaciones afines', afirma el informe elaborado por el comité del Senado que ha investigado las actividades de espionaje.
- "Millones de llamadas telefónicas, telegramas y comunicaciones por télex fueron revisados por la ANS. Los resultados de estas revisiones fueron enviados a la CIA, al FBI, al Servicio Secreto, a la Oficina de Narcóticos y a otros departamentos.
- "Desde 1945, la ANS obtuvo copias de todos los telegramas enviados o recibidos por conducto de las compañías [Radio Corporation of America] RCA e [International Telephone & Telegraph] ITT, y una selección de los transmitidos por Western Union."[53]
- "El informe de los senadores precisa que las actividades de la ASN se llevaron a cabo sin ningún tipo de autorización judicial. "[…] se informó que la Oficina Federal de Investigaciones (FBI) sigue instalando aparatos de escucha electrónicos en locales y domicilios privados, a pesar de la reglamentación que se opone a éstos métodos […]."[54]

[52] Gregorio Selser, NSC: National Security Council. NSA: National Security Agency. Agencias de Inteligencia militares de los Estados Unidos. 1960-1990, Fondo A, recortes y páginas de diarios, páginas de revistas, cables, clave de expediente: W US99, CAMENA, UACM, imagen 2/99.
[53] *Ídem.*
[54] *Ídem.*

Estas investigaciones fueron hechas por la Comisión de Inteligencia del Senado, presidida por el entonces senador del Partido Demócrata Frank Church. Se creó el Comité Selecto del Senado de Estados Unidos para el Estudio de las Operaciones Gubernamentales Respecto de las Actividades de Inteligencia. Los resultados de este comité concluyeron con la creación de una corte para otorgar permisos de escuchas con fundamento judicial promulgándose la Ley de Vigilancia de Inteligencia del Exterior de 1978, conocida como FISA.

El artículo "La Agencia de Seguridad de EU espía las comunicaciones desde hace 25 años". Fechada también el 11 de mayo de 1975, con información de [United Press International] UPI establece que "[…] alrededor de 75 ciudadanos estadunidenses cuyas comunicaciones estuvieron sujetas a intercepción, están en un archivo en las oficinas centrales de la NSA en Ft. Meade (Maryland). […] Muchas de las actividades de la NSA fueron reveladas durante las audiencias de la Comisión de Inteligencia del Senado […]".[55]

De acuerdo con lo expuesto, en la década de los setenta se sabía que las funciones de la NSA no sólo tenían como objetivo la recolección de información del extranjero, también había escuchas ilegales dentro de territorio estadunidense. Las escuchas se hacían bajo el concepto de Seguridad Nacional.

Ya entonces, otra función de la NSA era obtener información ventajosa para transacciones comerciales. En 1976 Tom Litterick, legislador del partido Laborista de Gran Bretaña, aseguró que las bases de la NSA en su país servían para el espionaje comercial. "[…] usan cuatro instalaciones militares británicas, en Edzell, Escocia; en Chicksands, Cheltenham y una en Hampshire para sintonizar las comunicaciones de organizaciones comerciales británicas".[56]

El espionaje industrial no es tema de este trabajo. Empero, vale la pena resaltar las declaraciones del referido legislador. La agencia británica de espionaje, Cuartel General de Comunicaciones del Gobierno *(Government Communications Headquarters,* GCHQ) continuó cooperando con la NSA. Tom Litterick expuso que "[…] las capacidades técnicas

[55]Gregorio Selser, NSC: National Security Council. NSA: National Security Agency. Agencias de Inteligencia militares de los Estados Unidos. 1960-1990, Fondo A, recortes y páginas de diarios, páginas de revistas, cables, clave de expediente: W US99, CAMENA, UACM, imagen 3/99.

[56] Gregorio Selser, "¿EU robando secretos?, Associeted Press, Londres, NSC: National Security Council. NSA: National Security Agency. Agencias de Inteligencia militares de los Estados Unidos. 1960-1990, Fondo A, recortes y páginas de diarios, páginas de revistas, cables, Clave de expediente: W US99, CAMENA, UACM, 2 de agosto de 1976, imagen 13/99.

estadunidenses son extremadamente inmensas. No hay código que esté a salvo, los estadunidenses pueden descifrar cualquier cosa. […] Cuando es cuestión de dinero, los estadunidenses no reconocen a nadie como sus amigos".[57]

1.1.2 Desglose de la actual Comunidad de Inteligencia

En la época contemporánea son diecisiete las agencias que componen a la Comunidad de Inteligencia. Se organizan de la siguiente manera de acuerdo con el departamento al que pertenecen:

> — Dos agencias independientes: la Oficina del Director de Inteligencia Nacional, ODNI y la Agencia Central de Inteligencia.
>
> — Ocho del Departamento de Defensa: Agencia de Seguridad Nacional; Oficina Nacional de Reconocimiento, NRO, por sus siglas en inglés; Agencia de Inteligencia Nacional Geoespacial, NGA, por sus siglas en inglés; y los elementos de Inteligencia de los cuatro elementos armados del Departamento de Defensa: el ejército, la marina, el cuerpo de marines y la fuerza aérea.
>
> — Siete elementos de otros departamentos y agencias: Departamento de Energía, DOE, por sus siglas en inglés; la Oficina de Inteligencia y Análisis del Departamento de Seguridad Interna, así como la Inteligencia de la Guardia Costera; la Oficina Federal de Investigaciones, la Oficina de Inteligencia y Seguridad Nacional de la Administración de Control de Drogas, ONSI-DEA, por sus siglas en inglés, ambas del Departamento de Justicia; la Oficina de Inteligencia e Investigación para el Departamento de Estado, INR, por sus siglas en inglés, y la Oficina de Inteligencia y Análisis del Departamento del Tesoro OIA, por sus siglas en inglés.[58]

A continuación se muestran tres cuadros sinópticos de elaboración propia, que permiten puntualizar la localización de las agencias de Inteligencia en la estructura estatal. Para fines prácticos sólo se muestran las siglas de algunas de ellas, no todas cuentan con acrónimos. El

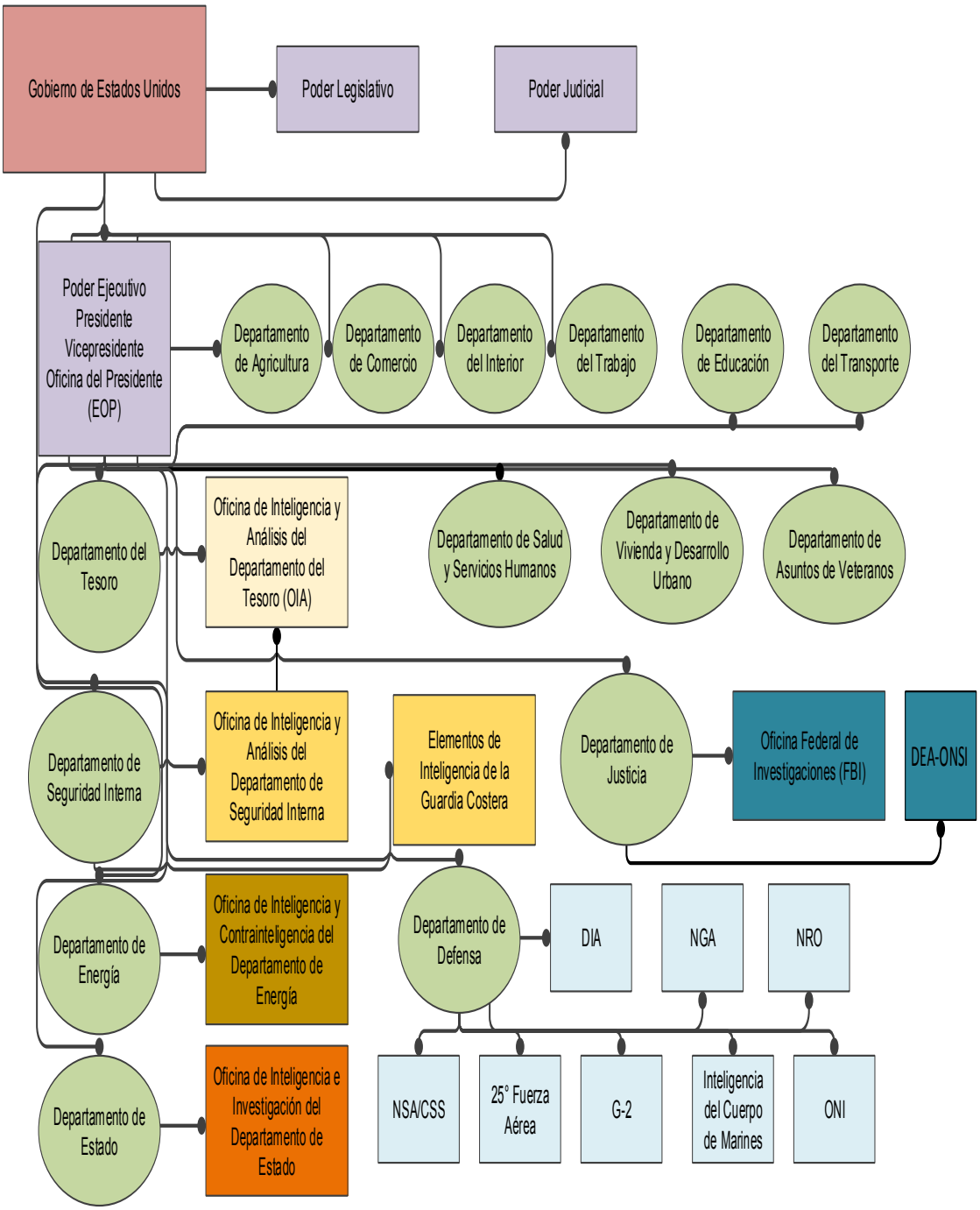
[57] *Ídem.*
[58] s/a, "Members of the IC", *Office of the Director of National Intelligence,* https://www.dni.gov/index.php/what-we-do/members-of-the-ic [traducción propia]

gobierno de Estados Unidos está dividido en tres poderes: Ejecutivo, Legislativo y Judicial. Las diecisiete agencias que conforman la Comunidad de Inteligencia responden al Poder Ejecutivo, y dentro de éste, la mayoría de ellas se encuentran bajo el Departamento de Defensa.

El primer cuadro sinóptico muestra a quince de ellas, con excepción de las dos que se catalogan como independientes. Éstas, las quince, se encuentran ligadas con el departamento del Poder Ejecutivo al que pertenecen.

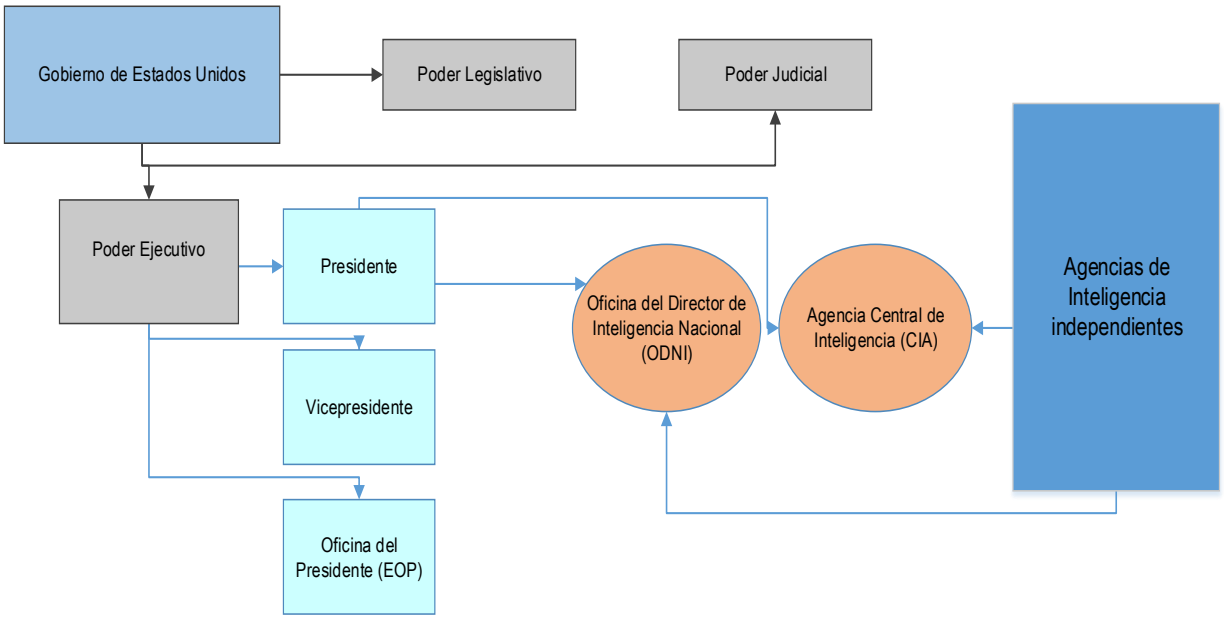
El segundo esquema muestra a las dos agencias independientes, la CIA y la ODNI. Independientes quiere decir que ambas responden al Poder Ejecutivo, mas no se encuentran dentro de la estructura del Departamento de Defensa.

Por último, el tercer esquema desglosa a las agencias de Inteligencia del Departamento de Defensa y el área a la que pertenecen.



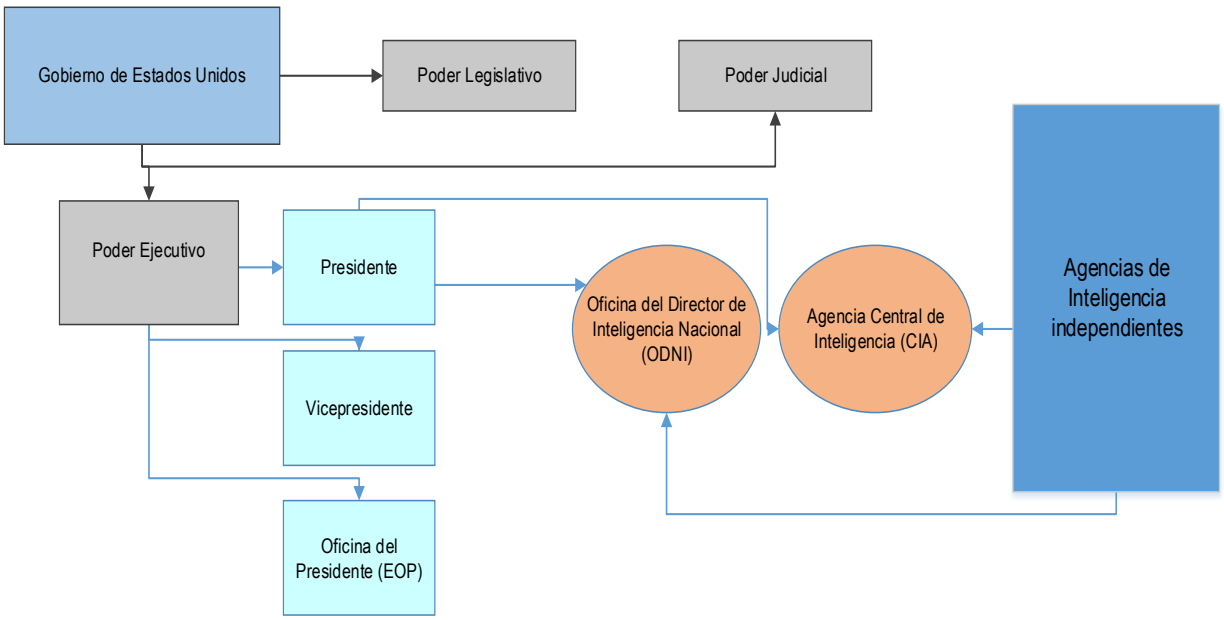
Cuadro de elaboración propia con información de: www.intelligencecareers.gov/icmembers.html

Esquema 1



Cuadro de elaboración propia con información de: www.intelligencecareers.gov/icmembers.html

Esquema 2



Cuadro de elaboración propia con información de: www.intelligencecareers.gov/icmembers.html

Esquema 3

Como vimos en los esquemas, las dos agencias independientes, CIA y ODNI, no pertenecen al área armada del gobierno. Cabe recordar que el jefe del Ejecutivo es también el jefe de las fuerzas armadas. Las funciones de las diecisiete agencias de Inteligencia son las siguientes:

1. Oficina del Director de Inteligencia Nacional. ODNI. Es la cabeza de la Comunidad de Inteligencia. La dirige el Director de Inteligencia Nacional. "El presidente selecciona al DNI con el consejo y aprobación del Senado." [59]

En diciembre de 2004 se reformó el Acta de Seguridad Nacional de 1947. Esta enmienda se dio a través de la Reforma de Inteligencia y el Acta de Prevención del Terrorismo, en ella se crea la Dirección de Inteligencia Nacional para coordinar a las diferentes agencias. La enmienda se hizo durante la presidencia de George W. Bush.

2. Agencia Central de Inteligencia, CIA. Es la encargada de proporcionar información de Inteligencia para garantizar la Seguridad Nacional. La información de Inteligencia que crea se la brinda a los políticos estadunidenses de mayor rango.

Agencias del Departamento de Justicia

3. Oficina Federal de Investigaciones, FBI. Es la agencia de Inteligencia responsable de identificar las amenazas a la Seguridad Nacional y de penetrar en las redes nacionales y transnacionales que tienen "el deseo y la capacidad de hacer daño" a Estados Unidos.
4. Oficina de Inteligencia y Seguridad Nacional de la Administración de Control de Drogas, ONSI-DEA. Se convirtió en miembro de la IC en 2006. Su objetivo es mejorar los esfuerzos de Estados Unidos para reducir la oferta de drogas, proteger la Seguridad Nacional y luchar contra el terrorismo global. La DEA cuenta con 21 divisiones de campo en Estados Unidos, además de 80 oficinas en más de 60 países en el mundo.

Departamento del Tesoro

5. Oficina de Inteligencia y Análisis del Departamento del Tesoro, OIA. Se estableció por la Ley de Autorización de Inteligencia para el año fiscal 2004. Es responsable de la recepción, análisis, recopilación y difusión de la Inteligencia extranjera y la información de contraespionaje del extranjero relacionada con el funcionamiento y las responsabilidades del Departamento del Tesoro.

[59] s/a, "Who we are", Office of the Director of National Intelligence, https://www.dni.gov/index.php/who-we-are [traducción propia]

Agencias del Departamento de Seguridad Interna

6. Oficina de Inteligencia y Análisis del Departamento de Seguridad Interna. Es responsable del uso de la información obtenida de múltiples fuentes para identificar y evaluar las amenazas actuales y futuras a la Inteligencia nacional.
7. Inteligencia de la Guardia Costera. Se convirtió en miembro de la Comunidad de Inteligencia en diciembre de 2001. Entre sus responsabilidades se incluye la seguridad marítima y la protección del mar.

Departamento de Energía

8. Oficina de Inteligencia y Contrainteligencia del Departamento de Energía. Es responsable de las actividades de espionaje y contraespionaje del complejo del Departamento de Energía. Incluye cerca de treinta oficinas en el ámbito nacional encargadas de estas actividades.

Departamento de Estado

9. Oficina de Inteligencia e Investigación del Departamento de Estado. Le brinda al secretario de Estado información y análisis de eventos globales, así como análisis en tiempo real de Inteligencia de todas las fuentes.

Agencias de Inteligencia del Departamento de Defensa

10. Agencia de Espionaje del Departamento de la Defensa, DIA. Es la agencia de apoyo del Departamento de la Defensa. Se distingue por su importante producción y dirección de la Inteligencia militar en el extranjero. Proporciona información militar a los combatientes y responsables de la política de defensa. La DIA apoya la planificación militar y las operaciones para la adquisición y sistemas de armas.
11. Agencia de Seguridad Nacional y Servicio Central de Seguridad, NSA/CSS. Coordina, dirige y realiza actividades altamente especializadas para proteger los sistemas de información de Estados Unidos y producir señales para obtener Inteligencia del extranjero.
12. Agencia de Inteligencia Nacional Geoespacial, NGA. Proporciona Inteligencia geoespacial en apoyo a los objetivos de Seguridad Nacional. Contribuye a la preparación de las fuerzas militares estadunidenses.
13. Oficina Nacional de Reconocimiento, NRO. Diseña, construye y opera los satélites de

reconocimiento. Los productos de la NRO tienen una lista creciente de clientes, que incluyen a la CIA y al Departamento de Defensa. Sus investigaciones pueden advertir de posibles focos de conflicto en todo el mundo, ayudar a las operaciones militares y monitorear el medio ambiente. Se financia a través del Programa Nacional de Reconocimiento, que forma parte del Programa Nacional de Inteligencia Exterior.

14. Inteligencia del Ejército de Estados Unidos, también conocida como G-2. Es responsable de formular políticas, planificación, programación, presupuesto, gestión, supervisión del personal, evaluación y supervisión de las actividades de Inteligencia para el Ejército.
15. Oficina de Inteligencia Naval, ONI. Es proveedora líder de Inteligencia marítima de la Armada de Estados Unidos y de otros consumidores de la Comunidad de Inteligencia. ONI es la mayor organización de Inteligencia Naval con la mayor concentración de población civil. La mayor parte de la Inteligencia Naval comprende personal militar en servicio activo que se encuentra en todo el mundo.
16. Inteligencia del Cuerpo de Marines. Produce Inteligencia táctica y operativa para el apoyo en campos de batalla. Se encuentran todos los profesionales de Inteligencia de infantería de marina, responsables de la política, planes, programas, presupuestos y la supervisión del personal de Inteligencia y actividades de apoyo en la infantería de marina.
17. Agencia de Inteligencia, vigilancia y reconocimiento de la Fuerza Aérea de Estados Unidos, USAF-ISR, o la 25ª Fuerza Aérea. Su misión es entregar información ventajosa a los comandantes con el fin de alcanzar efectos cinéticos y no cinéticos contra objetivos en cualquier lugar del mundo, en apoyo a los requerimientos en operaciones tácticas y estratégicas. Su lema es: Libertad a través de la vigilancia.[60]

Las agencias de Inteligencia tienen como principal objetivo la Seguridad Nacional. El Departamento de Defensa define Seguridad Nacional como "concepto global que abarca tanto la defensa nacional como las relaciones exteriores de Estados Unidos con el propósito de obtener: a. beneficio o ventaja militar o de defensa sobre cualquier nación o grupo de naciones

[60] "About us", 25th Air Force, http://www.25af.af.mil/About-Us/History/

extranjeras; b. una posición favorable en las relaciones exteriores; o c. una postura defensiva capaz de resistir acciones hostiles o destructivas, internas o externas, cubiertas o encubiertas"[61].

Para cerrar con la estructura de la Comunidad de Inteligencia, se nombra a las cabezas de los departamentos y agencias de Inteligencia en relación directa con los programas de vigilancia masiva que se desarrollan en la última parte del capítulo. Corresponden a los gobiernos de George W. Bush y de Barack H. Obama.

George W. Bush fue el presidente de Estados Unidos número cuarenta y tres. Gobernó durante dos periodos, de 2001 a 2009. Richard B. Cheney fue el vicepresidente durante su Presidencia. El secretario de Defensa fue Robert M. Gates; la Secretaría de Estado estuvo a cargo de Condolezza Rice; el secretario de Energía fue Samuel W. Bodman; el secretario de Seguridad Interna, Michael Chertoff, y el fiscal general del Departamento de Justicia fue Michael Mukasey.[62]

Barack H. Obama fue el presidente número cuarenta y cuatro de Estados Unidos. Estuvo en el cargo por dos periodos que abarcaron de 2009 a 2017. Su gabinete estuvo compuesto por Joseph R. Biden como vicepresidente. El secretario de Defensa fue Ashton Carter; la Secretaría de Estado estuvo a cargo de Hillary R. Clinton hasta que renunció para ser la candidata del Partido Demócrata a la Presidencia, la sucedió John Kerry; el secretario de Energía fue Ernest Moniz; el secretario de Seguridad Interna Jeh Johnson y la fiscal general fue Loretta E. Lynch.[63]

Sin embargo, los cargos de las agencias de Inteligencia no necesariamente responden al cambio del titular del Poder Ejecutivo. "En febrero de 2005, el presidente [George W. Bush] nominó a John D. Negroponte, quien en ese entonces era embajador en Irak, como el primer director de Inteligencia nacional, y al teniente general de la fuerza aérea, Michael V. Hayden, como el vicesecretario adjunto DNI".[64] En 2007, John Michael McConnell, vicealmirante de la marina fue elegido como el segundo director de Inteligencia nacional hasta 2009 cuando le sucedió Dennis. C. Blair, almirante retirado del ejército. Dennis C. Blair ocupó el puesto por un

[61] National security**,** *Dod Dictionary of Military and Associated Terms*, as of August 2017, p. 162. [traducción propia]
[62]"President Bush's Cabinet", The White House, President George W. Bush, https://georgewbush-whitehouse.archives.gov/government/cabinet.html
[63] Para más información de otros puestos del gabinete, visitar https://obamawhitehouse.archives.gov/administration/cabinet
[64] "History", Office of the Director of National Intelligence, https://www.dni.gov/index.php/who-we-are/history [traducción propia]

breve periodo, y en agosto de 2010 fue reemplazado por el teniente general de la fuerza aérea, James R. Clapper. El quinto y actual director es Daniel Ray Coats, quien llegó a la cabeza de la ODNI en 2017. En 2011 perteneció al Comité Selecto del Senado en Inteligencia.[65]

Durante los gobiernos de George. W. Bush y Barak H. Obama hubo dos directores de la NSA: el teniente general Michael V. Hayden, quien ocupaba el cargo desde 1996, y desde 2006 el general Keith B. Alxander, quien provenía del ejército. A partir de 2014, la dirección cambió al almirante Michael S. Rogers, quien continúa en el cargo. El director de la NSA es, al mismo tiempo, el comandante del cibercomando de Estados Unidos y el jefe del Servicio de Seguridad Central.

El director de la CIA hasta 2005 estaba también encargado de la dirección de la comunidad de Inteligencia. A partir de la reforma a los servicios de Inteligencia y la creación de la Dirección de Inteligencia Nacional, el director de la CIA sólo se encargaría de supervisar las funciones de esta agencia. Peter Johnston Goss, nombrado por el presidente George W. Bush en 2004, fungió como director hasta 2006. Le sucedió en el cargo Michael V. Hayden hasta 2009, luego Leon Eward Panetta hasta 2011, David Patraeus hasta 2012 y John Brennan hasta enero de 2017. El actual director es Mike Pompeo.

Durante el periodo de ambos gobiernos, el FBI estuvo a cargo de dos directores: de 2001 a 2013 fue Robert S. Mueller III. De 2013 a 2017 el director fue James B. Comey y, a partir de agosto de 2017, el director es Christopher Wray.

Antes de comenzar el siguiente apartado es necesario explicar cómo surge el cibercomando de Estados Unidos, USCYBERCOM. Nace el 31 de octubre de 2010, tiene su sede en Fort Meade, Maryland y su principal comandante es, también, el director de la NSA. El actual jefe es el almirante Michael S. Rogers. Su misión es "[…] planear, coordinar, integrar, sincronizar y conducir actividades para: dirigir las operaciones y defensa de redes informáticas especificas del Departamento de Defensa, y preparar, dirigir y conducir todas las operaciones ciberespaciales del espectro militar en orden para llevar a cabo acciones en todos los dominios y asegurar que Estados Unidos y sus aliados tengan libertad de acción en el espacio cibernético

[65] Para mayor información, consultar la página oficial de la Oficina del Director de Inteligencia Nacional: www.dni.gov/index.php/who-we-are

y denegarle la misma a sus adversarios".[66] El USCYBERCOM, es una subunidad del Comando Estratégico de Estados Unidos[67] que, a su vez, forma parte de los nueve Comandos Combatientes Unificados.

Fuente: Departamento de Defensa de Estados Unidos[68]

1.2 Marco jurídico de la Comunidad de Inteligencia

Estados Unidos cuenta con tres documentos fundacionales: la Declaración de Independencia, la Constitución y la Carta de Derechos. A estos documentos se les conoce como Cartas de Libertad *(Charts of Freedom)*. La Carta de Derechos se compone con las primeras diez enmiendas a la Constitución, "define los derechos de los ciudadanos y los estados en relación con el gobierno."[69] La primera parte de la Constitución se enfoca en la estructura del gobierno federal, mientras la Carta de Derechos fue creada para dar confianza a los ciudadanos respecto de su gobierno. La cuarta enmienda forma parte de estas primeras diez enmiendas.

Por debajo de las Cartas de Libertad se localiza el Código Federal de Leyes de Estados Unidos (*U.S Code*, *U.S.C)*. Este compendio de leyes contiene la legislación federal recopilada.

---

[66] "Mission", U.S. Cyber Command (USCYBERCOM), http://www.stratcom.mil/Media/Factsheets/Factsheet-View/Article/960492/us-cyber-command-uscybercom/, última actualización, 30 de septiembre de 2016. [traducción propia]
[67] En inglés: *U.S Strategic Command*.
[68] "Commanders'Area of Responsibility", U.S Department of Defense, https://www.defense.gov/About/Military-Departments/Unified-Combatant-Commands/
[69] s/a, "The bill of rights: a transcription", America´s Founding Documents, National Archives, https://www.archives.gov/founding-docs/bill-of-rights-transcript [traducción propia]

Está compuesto por cincuenta y cuatro títulos[70], y cada título puede contener varias secciones.

Las leyes que proporcionan el marco jurídico de la Comunidad de Inteligencia se encuentran en esta legislación. Este marco le da validez institucional y le permite desempeñar sus funciones con legalidad. Como hemos visto, la Comunidad de Inteligencia, desde la segunda posguerra hasta las reformas en materia de seguridad surgidas a partir del 11 de septiembre de 2001 ha crecido, se han creado nuevas agencias más especializadas y con más funciones; como consecuencia, la normatividad ha variado, y por tal razón se han realizado numerosas enmiendas.

En este apartado se abarca desde el Acta de Seguridad Nacional de 1947, legislada en las postrimerías de la Segunda Guerra Mundial, hasta las últimas enmiendas a la Ley FISA, legislada después de los conocidos escándalos de Watergate.

Antes de dar paso al apartado sobre normatividad, conviene recordar en qué consistió el escándalo Watergate. Cabe entonces señalar que a principios de los años setenta del siglo pasado ocurrió un suceso de tal importancia política, que concluyó con la creación de una corte para controlar el espionaje interno. El famoso caso cimbró a Estados Unidos y ocasionó la renuncia del presidente Richard M. Nixon. "El asunto de Watergate comenzó durante la campaña presidencial de junio de 1972, cuando arrestaron a cinco ladrones provistos de material para realizar escuchas ilegales y equipo fotográfico, tras ser sorprendidos en el momento de entrar en las oficinas del Comité Demócrata Nacional, en el complejo de apartamentos de Watergate, en Washington".[71]

Este caso evidenció el uso del espionaje para fines políticos personales o de grupo en el sistema de partidos. El objetivo era escuchar las conversaciones del Partido Demócrata en el marco de las elecciones en las que R. Nixon buscaba la reelección presidencial por el Partido Republicano "[…] uno de los cinco [detenidos], James McCord, Jr., trabajaba para la campaña de Nixon; era agente de 'seguridad' al servicio del Comité de Reelección del presidente (CREEP). Otro de los cinco ladrones llevaba una agenda en la que aparecía el nombre de E. Howard Hunt, cuya dirección era la Casa Blanca. Hunt era ayudante de Charles Colson,

[70] "U. S. Code: Table of Contents", Cornell Law School. Legal Information Institute, https://www.law.cornell.edu/uscode/text

[71] Howard Zinn, Toni Strubel (trad.), "Los años setenta: ¿Bajo control?", *La otra historia de los Estados Unidos (desde 1492 hasta hoy)*, Capítulo 20, México, D.F., Siglo XXI, p. 402.

consejero especial del presidente Nixon"[72].

Regresemos al marco legal que dará sentido al resto de la investigación. Las leyes que a continuación se describen no son todas las que estructuran a la Comunidad de Inteligencia; abarcarlas en su totalidad sería motivo de un solo estudio. Aquí sólo se alude a las relativas a la formación de la IC, al espionaje electrónico y a las filtraciones.

1.2.1 Ley de Espionaje

La ODNI publicó, en el verano de 2016, la última versión del *Libro de referencias legales de la Comunidad de Inteligencia.* [73] En ese volumen, que recopila todas las leyes que dan sentido a la Comunidad de Inteligencia, no se encuentra la Ley de Espionaje, aunque bajo ella han sido juzgados todos los filtradores de la historia reciente. Esta ley, promulgada en abril de 1917, en el contexto de la Primera Guerra Mundial, firmada por el entonces presidente Woodrow Wilson, se tituló: "Una ley para castigar actos que interfieran con las relaciones exteriores, la neutralidad y el comercio exterior; castigar el espionaje y reforzar las leyes criminales de los Estados Unidos, y para otros propósitos". En el presente, la Ley de Espionaje se encuentra en el Código de Leyes Federales, Título 18 Crímenes y Procedimientos Criminales, Parte I, Capítulo 37, secciones 793, 794, 795, 796, 797, 798 y 798A.[74]

La sección 798, se refiere a la divulgación de información.

> Título 18- Crímenes y procedimientos criminales
>
> Parte I-Crímenes
>
> Capítulo 37- Espionaje y censura
>
> SS 798- Divulgación de información clasificada
>
> (a) Quienquiera que deliberada y voluntariamente comunique, suministre, transmita, o de otra manera ponga a disposición de una persona no autorizada; o publique, o use de cualquier manera perjudicial a la seguridad o interés de Estados Unidos, o para el beneficio de cualquier gobierno extranjero para el detrimento de Estados Unidos,

[72] *Ídem.*
[73] s/a, *Intelligence Community Legal Reference Book,* Office of the Director of National Intelligence, Office of General Counsel, Summer 2016, 1023 pp.
[74] Se pueden consultar en: https://www.law.cornell.edu/uscode/text/18/part-I/chapter-37

cualquier información clasificada.[75]

(1) relativo a la naturaleza, preparación o uso de cualquier código, cifra, o sistema criptográfico de Estados Unidos o de cualquier gobierno extranjero; o

(2) relativo al diseño, construcción, uso, mantenimiento o reparación de cualquier dispositivo, equipo, o aparato usado o preparado para uso de Estados Unidos o de cualquier gobierno extranjero para propósitos de Inteligencia criptográfica o de las comunicaciones; o

(3) relativo a las actividades de Inteligencia de las comunicaciones de Estados Unidos o de cualquier gobierno extranjero; o

(4) obtenido por el proceso de Inteligencia de la comunicación de las comunicaciones de cualquier gobierno extranjero, a sabiendas que lo mismo ha sido obtenido por tal proceso

Será penalizado bajo este título o encarcelado no más de diez años, o los dos.[76]

"Inicialmente, la Ley [de espionaje] se usó contra activistas pacifistas y espías extranjeros. Desde la década de los setenta, la ley ha sido reinterpretada como una amplia ley antifiltraciones, que prohíbe compartir información clasificada con nadie, por ninguna razón".[77]" Tal es el caso de la entrega de información a periodistas.

1.2.2 Acta de Seguridad Nacional de 1947

El Acta de Seguridad Nacional de 1947, cuyo título completo es "Una ley que promueve la Seguridad Nacional al proveer una Secretaría de Defensa; el establecimiento de un sistema militar nacional, un Departamento del Ejército, un Departamento de la Marina y un Departamento de la Fuerza Aérea; y para la coordinación de las actividades del sistema militar nacional con otros departamentos y agencias del gobierno concernientes a la Seguridad

[75] La interpretación para información clasificada del Diccionario de términos del DoD se encuentra en el glosario. Sin embargo, la Ley de Espionaje define su propia interpretación de información clasificada: significa información que, al tiempo de la violación de esta sección [18 USC SS 798], es, por razones de Seguridad Nacional, específicamente designada por una agencia del gobierno de Estados Unidos, como de diseminación y distribución limitada.

[76] 18 USC SS 798-Disclousure of classified information, U.S. Code, Title 18, Part I, Chapter 37, SS 798, Legal Information Institute, Conell Law School, https://www.law.cornell.edu/uscode/text/18/794 [traducción propia]

[77] Peter Sterne, "How the Espionage Act morphed into a dangerous tool used to prosecute sources and threaten journalists", Freedom of the Press Foundation, II/III, https://freedom.press/news/how-espionage-act-morphed-dangerous-tool-used-prosecute-sources-and-threaten-journalists/ [traducción propia]

Nacional"[78], configura la Comunidad de Inteligencia.

Su objetivo fue lograr una mayor reorganización de la política exterior y militar. En la página de internet del Departamento de Estado[79], se arguye que la creación de esta ley obedeció a la necesidad de lograr una mayor integración de las agencias de espionaje. La ley conforma al Consejo Nacional de Seguridad *(National Security Council, NSC)*, el cuál será el antecesor de la Comunidad de Inteligencia; continúa en funciones precedido por el presidente, el asesor de Inteligencia es el Director de Inteligencia Nacional. Además, se instituyó la Secretaría de Defensa, la CIA y la figura del director central de Inteligencia (DCI, por sus siglas en inglés) que a su vez era el director de la CIA.

Desde otra perspectiva, esta ley surge por la necesidad de darle contenido al concepto de Seguridad Nacional. "Su objetivo, explica ante el Congreso el secretario de Marina James Forrestal, es el de 'permitir la coordinación de las tres ramas de las fuerzas armadas (la Marina, las fuerzas aéreas y el ejército de tierra) y, lo que me parece más importante aún, la articulación entre política exterior y la política nacional, la integración de nuestra economía civil con los imperativos militares; permitir un progreso constante en el ámbito de la investigación y la ciencia aplicada.'"[80]

Es en este momento donde se incorpora al lenguaje militar el término de Seguridad Nacional como "la convergencia de las distintas armas, […] en relación con este tema en el que, ya en 1945, la referencia de Seguridad Nacional se incorpora a la reflexión de los 'planificadores militares', por instigación del jefe de Estado Mayor, el general George C. Marshall, futuro secretario del Departamento de Estado del presidente Truman y promotor del plan de ayuda para la reconstrucción de Europa."[81] Esta ley fue firmada por Harry S. Truman. Se encuentra en el Código Federal de Leyes, Título 50. Guerra y Defensa Nacional.

1.2.3 Acta de la Reforma de Inteligencia y Prevención del Terrorismo de 2004

Esta ley constituye una reforma al Acta de Seguridad Nacional de 1947. Su título completo es el siguiente: Acta para reformar a la comunidad de Inteligencia y las actividades relacionadas

[78] s/a, *Intelligence Community Legal Reference Book, op. cit.,* p. 26.
[79] s/a, "National Security Act of 1947", Office of the Historian, 1945-1952, Milestones, https://history.state.gov/milestones/1945-1952/national-security-act
[80] Armand Mattelart, Mattelart Armand, Gilles Multigner (trad.), Un mundo vigilado, Barcelona, Paidós, 2009, p. 70.
[81] *Ídem.*

con la Inteligencia del gobierno de Estados Unidos, y para sus propósitos;[82] IRTPA, por sus siglas en inglés. Fue firmada en diciembre de 2014 por el entonces presidente Barack Obama. En esta reforma se determinó la función de un director central de Inteligencia y se creó la Oficina del Director de Inteligencia Nacional. Además,

- Reorganizó a la Comunidad de Inteligencia, creó el cargo de director de Inteligencia Nacional para servir al presidente como asesor en jefe de Inteligencia y de cabeza de la IC, además de asegurar una coordinación más cercana e integrar a las dieciséis agencias [que, en ese entonces,] formaban a la IC.
- Se estableció el Centro Nacional de Contraterrorismo, NCTC, por sus siglas en inglés.
- Se estableció el Consejo de Supervisión de la Privacidad y Libertades Civiles, PCLOB, por sus siglas en inglés.
- Mejoró las capacidades del FBI. [Permisos de escuchas ilegales sin orden judicial]
- Adopción de la orden ejecutiva 13,356, la cual se refiere al fortalecimiento del intercambio de información entre agencias.
- Se estableció el Consejo de Intercambio de Información, ISC, por sus siglas en inglés.[83]

Es en esta enmienda a la Ley de Seguridad de 1947, dentro del título para mejorar las capacidades de actuación y respuesta del FBI, donde se autorizan las escuchas telefónicas y las búsquedas secretas de individuos sospechosos de terrorismo que no tengan conexión con un poder extranjero. Para lograr esto también se modificó la Ley FISA de 1978.

1.2.4 Ley de la Agencia de Seguridad Nacional de 1959

Esta ley se encuentra en el Título 50, Capítulo 47; abarca de las secciones 3601 a la sección 3618, del Código Federal de Leyes de Estados Unidos. Nos detenemos en esta ley porque en ella se dejan ver ciertos comportamientos de secrecía que rodean la actuación de la NSA. Por

[82] s/a, *Intelligence Community Legal Reference Book*, op.cit., p. 193. [traducción propia]
[83] s/a, "The Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA)", Privacy & Civil Liberties, Justice Information Sharing, https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1282

ejemplo, no hay información concreta acerca del número de empleados que trabajan para la NSA. Lo más que se puede encontrar son estimaciones que varían de autor a autor, lo cual se explica porque, en la sección 3605 del U.S.C se establece que "[…] nada en esta acta o cualquier otra ley […] estará hecha para que se pueda requerir la divulgación de la organización o cualquiera otra función de la Agencia de Seguridad Nacional, o cualquier información con respecto a las actividades de la misma, los nombres, títulos, salarios o número de personas empleadas por esta agencia".[84] Sobre las actividades realizadas por la agencia, la sección 3608 nos da una buena idea.

50 U.S.C SS 3608

(a) El director de la Agencia de Seguridad Nacional deberá organizar y prescribir regulaciones concernientes a idiomas y programas de entrenamiento en idiomas para personal criptológico civil y militar. Al establecer programas bajo esta sección para idiomas y entrenamiento en idiomas, el director…

(1) en lo relativo al entrenamiento y las instrucciones deberá proveer especializaciones como las funcionales y geográficas.

(2) puede arreglar entrenamiento e instrucciones mediante otras agencias del gobierno, y en caso de que el entrenamiento apropiado o las instrucciones no estén disponibles a través de las instalaciones del gobierno, podrán ser suministradas por instalaciones no gubernamentales útiles en los campos de idiomas y relaciones exteriores;

(3) podrá apoyar programas que suministren habilidades lingüísticas; en caso de que estos programas no puedan ser brindados por el gobierno, se obtendrá el apoyo a través de acuerdos, subvenciones y cooperación con instituciones educativas no gubernamentales; y

(4) puede obtener, por designación o acuerdo, los servicios de individuos como maestros de idiomas, lingüistas o proyectos especiales de idiomas a personal.[85]

(b) […]

(c) en la medida en que no sea incompatible con la opinión del secretario de Defensa, con

[84] s/ a, *Intelligence Community Legal Reference Book*, op. cit., p. 275. [traducción propia]
[85] *Ibíd.,* p. 277. [traducción propia]

la operación de la reserva de unidades militares criptográficas y en orden de mantener las necesarias capacidades en habilidades de lenguas extranjeras y habilidades necesarias para la Agencia de Seguridad Nacional, el director puede establecer una reserva lingüística criptológica.

50 U.S.C SS 3610

(a) (1) El secretario de la Defensa (o quien éste designe) puede, por regulación, establecer una plantilla para un sistema de empleados criptólogos civiles especializados dentro de la Agencia de Seguridad Nacional, que será conocido como Servicio Ejecutivo Principal Criptológico.

50. U.S.C SS 3611

(a) El director de la Agencia de Seguridad Nacional puede realizar subvenciones a individuos e instituciones del sector privado para conducir la investigación criptográfica. […] El director debe determinar que la concesión de la subvención será claramente consistente con la Seguridad Nacional.

50 U.S.C. SS 3614

(a) El propósito de esta sección es establecer un progrgama de entrenamiento estudiantil, que conduzca al grado de bachillerato, para facilitar el reclutamiento de individuos, particularmente a una minoría de estudiantes de preparatoria que hayan demostrado capacidad para desarrollar habilidades críticas a la misión de la Agencia de Seguridad Nacional, incluidas matemáticas, informática, ingeniería y lenguas extranjeras.

(b) El secretario de la Defensa está autorizado, de forma discrecional, a asignar empleados civiles de la Agencia de Seguridad Nacional como estudiantes acreditados en instituciones profesionales, técnicas o de alto nivel de aprendizaje para entrenarse en el nivel universitario en habilidades críticas para el efectivo desempeño de la misión de la agencia.[86]

1.2.5 Ley de vigilancia del espionaje del extranjero de 1978

La ley de vigilancia del espionaje del extranjero de 1978, FISA, por sus siglas en inglés, fue promulgada junto con el tribunal especializado en resolver los requerimientos para obtener o

[86] *Ibíd.,* pp. 277-284. [traducción propia]

denegar permisos de espionaje; esto quiere decir: la autorización judicial para realizar escuchas, seguimiento e incluso decomiso de pertenencias.

El título completo de esta ley es: "Una ley para autorizar la vigilancia electrónica para la obtención de información de Inteligencia extranjera".[87] Se encuentra en el título 50 del U.S.C Guerra y Defensa Nacional, Capítulo 36. Está divida en ocho títulos: I. Vigilancia electrónica dentro de Estados Unidos para propósitos de Inteligencia del extranjero; […] III. Registros físicos dentro de Estados Unidos para propósitos de Inteligencia del extranjero; IV. *Pen registers* y *trap and trace devices*[88] para propósitos de Inteligencia extranjera; V. Acceso a ciertos registros de negocios por propósitos de Inteligencia del extranjero. VI. Supervisión; VII. Procedimientos adicionales respecto de ciertas personas fuera de Estados Unidos y VIII. Protección a personas que ayuden al gobierno.[89]

La ley promulgó la creación de la Corte para la Vigilancia del Extranjero o FISC, por sus siglas en inglés. Ésta se describe, a sí misma, como el "Tribunal especial autorizado por el juez máximo de la Suprema Corte de Estados Unidos *(Chief Justice of the United States*) para obtener órdenes relacionadas con las investigaciones en Seguridad Nacional".[90]

En la página de internet del Departamento de Justicia de Estados Unidos, en su sección "Intercambio de información acerca de la impartición de la justicia: Departamento de Justicia, Oficina de programas judiciales y la Oficina de asistencia judicial *(Justice Information Sharing U.S. Department of Justice, Office of Justice Programs, Bureau of Justice Assistance)",* se precisa que FISA es "la legislación resultado de investigaciones del Congreso a las actividades de espionaje federales realizadas en nombre de la Seguridad Nacional. Mediante FISA, el

[87] *Ibíd.,* p. 416. [traducción propia]

[88] *Pen registers and trap and trace devices;* en el Título 18 del U.S.C. sección 3127. El término *pen register* se entiende como "el dispositivo o proceso que graba o decodifica el marcado, enrutamiento, direccionamiento o señalización de información transmitida por un instrumento o instalación, de donde comunicaciones alámbricas o electrónicas son transmitidas, proporcionadas. Sin embargo, dicha información no incluirá los contenidos de ninguna comunicación. Dicho mandato no incluye ningún aparato o proceso usado por un proveedor o cliente de un servicio de comunicación alámbrico o electrónico para facturación o grabación de un incidente de facturación para servicios de comunicación proporcionados por dicho proveedor o por ningún aparato o proceso usado por un proveedor o cliente de servicios de comunicaciones alámbricas para contabilidad de costes u otros propósitos en el cauce ordinario de sus negocios. […] El término *trap and trace device* significa un aparato o proceso, el cual captura la entrada de impulsos electrónicos u otros impulsos que identifican el origen del número de marcado, enrutamiento, de destino e información de señalización que, muy probablemente, identifique la fuente de una comunicación electrónica, siempre y cuando dicha información no incluya los contenidos de la comunicación. [traducción propia]

[89] s/a, *Intelligence Community Legal Reference Book*, *op. cit.,* pp. 416-418. [traducción propia]

[90] "The Foreign Intelligence Surveillance Act of 1978 (FISA)", Justice of Information Sharing , U.S. Department of Justice, Office of Justice Programs, Bureau of Justice Assitance, https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1286 [traducción propia]

Congreso buscó proveer vigilancia judicial y del Congreso a las actividades de espionaje de Inteligencia extranjera mientras se mantiene la secrecía necesaria para el monitoreo de las amenazas a la Seguridad Nacional. FISA (...) establece los procedimientos para el espionaje físico y electrónico y la recolección de información de Inteligencia extranjera".[91]

Sin embargo, en el reporte del Servicio de Investigación del Congreso de Estados Unidos *(Congressional Research Service),* intitulado "La Ley de vigilancia del espionaje del extranjero: una visión general del marco legal y del Tribunal de vigilancia del espionaje del extranjero y del Tribunal para las revisiones de órdenes del Tribunal de vigilancia del espionaje del extranjero"[92], se dice que "las investigaciones cuyo propósito sea obtener información derivada del espionaje del extranjero, dan pie a una tensión entre los intereses de Seguridad Nacional legítimos del gobierno y la protección de los intereses privados."[93] La Cuarta Enmienda de la Constitución de Estados Unidos establece "el derecho de los individuos a la seguridad de su persona, sus hogares, sus escritos y sus pertenencias personales, en contra de registros e incautaciones irrazonables; este derecho será inviolable y no se expedirá ninguna orden más que cuando exista causa probable, apoyada por juramento o protesta, y se describa de forma particular el lugar que deba ser registrado y las personas que deban ser detenidas o las cosas que hay que incautar".[94]

La legislación fue promulgada en respuesta al reporte del Comité Selecto del Senado para el estudio de operaciones gubernamentales concernientes a actividades de espionaje *(Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities the Church Committee)*, conocido como Comité Church, ya mencionado. Éste pormenorizó las denuncias de abusos de autoridad del Poder Ejecutivo para llevar a cabo espionaje electrónico doméstico, en supuesto interés de la Seguridad Nacional y, también, en respuesta a la sugerencia de la Corte Suprema, a partir de un caso de 1972, el cual sugería que bajo la Cuarta Enmienda se haría necesario algún tipo de orden judicial para llevar a cabo las

[91]"The Foreign Intelligence Surveillance Act of 1978 (FISA)", Justice of Information Sharing, *op. cit.*

[92]En inglés:*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*

[93]Elizabeth B. Bazan, Legislative Attorney, American Law Division, "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. Updated February 15, 2007", CRS Report for Congress, Prepared for Members and Committes of Congress, Congressional Research Service, p.6. [traducción propia]

[94] *Ibíd.*, notal al pie de página, p.6. [traducción propia]

investigaciones relacionadas con la Seguridad Nacional. En 1978, el presidente de Estados Unidos era Jimmy Carter, quien junto con el Senado aprobó la ley. El tribunal está localizado dentro del Departamento de Justicia.

El abogado constitucionalista y periodista estadunidense Glenn Greenwald, en su artículo publicado en el periódico *The Guardian* bajo el título "La supervisión judicial de FISA: una mirada al interior de un proceso secreto y vacío" *(Fisa court oversight: a look inside a secret and empty processes),* apuntaló que al promulgarse la Ley FISA, en 1978, el principal propósito fue asegurar la prohibición al gobierno de Estados Unidos de vigilar las comunicaciones electrónicas de los ciudadanos estadunidenses si no se obtenía una orden individualizada para requerir que se demuestre la causa probable (por la que se supone) que la persona que será espiada es agente de un poder extranjero o de una organización terrorista.

Después del atentado del 11 de septiembre de 2001, el entonces presidente de Estados Unidos, George W. Bush, emitió una orden ejecutiva en la que permitió que la NSA "[… violara], de manera reiterada", la Ley de Vigilancia de Inteligencia Exterior de 1978. "La administración Bush se declaró competente para hacer esto a tenor de una Ley de emergencia aprobada por el Congreso: la Autorización para el Uso de la Fuerza Militar y la Ley Patriota, que fue secreta hasta que en 2005 el diario *The New York Times* reveló su existencia".[95]

1.2.6 Enmienda Patriota

Después de los atentados del 11 de septiembre de 2001, se legisló la enmienda a FISA, conocida como Enmienda Patriota *(Patriot Act).* En ésta se "regula" el espionaje a las comunicaciones. Esto, a causa de la "decisión del Congreso, después del 11 de septiembre, de realizar enmiendas a la ley FISA, a través de la Enmienda Patriota, [para] que FISA [autorizara y] controlara el espionaje electrónico durante la Guerra contra el Terror". [96]

El nombre completo de la Enmienda Patriota es "Unir y Fortalecer América al Proporcionar las Herramientas para Interceptar y Obstruir el Terrorismo", cuyo acrónimo en inglés es PATRIOT. La sección que a continuación se reproduce se encuentra en el U.S.C

[95] Julian Assange, María Maestro (trad.), *Cypherpunks. La libertad y el futuro de Internet*, México, D.F., Planeta Mexicana, 2013, pie de página no. 44, p. 64.
[96] Katherine L. Wong, "Recent Developments. The NSA Terrorist Surveillance Program", Harvard Journal on Legislation, 2006, Vol. 43, No. 2, pp. 524 y 525.

sección 403-5d, y fue una de las enmiendas de esta ley. Enmienda a la SS 403-5d,

> Consistente con la responsabilidad del director central de Inteligencia para proteger las fuentes y métodos de Inteligencia y la responsabilidad del fiscal general de proteger información delicada de los servicios de seguridad, será legal revelar información de una amenaza, un potencial ataque u otros actos graves y hostiles de un poder extranjero o un agente de poder extranjero, sabotaje doméstico o internacional, terrorismo doméstico o internacional, o actividades clandestinas de Inteligencia para recopilar información por un servicio de Inteligencia o red de un poder extranjero o agente de un poder extranjero, dentro de Estados Unidos u otro lugar, obtenido como parte de una investigación criminal, para ser divulgado o comunicado a los correspondientes oficiales de los gobiernos federal, estatales, locales o de gobiernos extranjeros, con la finalidad de prevenir o responder a dicha amenaza.
>
> Cualquier oficial que reciba información conforme a esta norma, sólo puede usar la información en los aspectos necesarios para la gestión de los deberes oficiales, sujeto, en cualquier caso, a los límites de la develación no autorizada de la información, y, cualquier oficial de un gobierno estatal, local o extranjero que reciba información relevante para esta ley sólo puede usar la información en concordancia con los lineamientos que el fiscal general y el director central de Inteligencia de forma conjunta emitan.[97]

¿Pero qué significa, en términos concretos, esta enmienda? La sección 215 del Acta Patriota aclara la pregunta. Se encuentra en el título 50 del U.S.C, en la sección 1861 llamada Acceso a ciertas grabaciones de negocios para investigaciones de Inteligencia extranjera e investigaciones internacionales de terrorismo que, a su vez, es una enmienda al Título V de la Ley FISA de 1978.

(a)Solicitud de orden; generalmente por conducto de una investigación

[97] U.S. Code, Title 50, Chapter 15, Subchapter I, sección 403-5d, Legal Information Institute, Cornell Law School, https://www.law.cornell.edu/uscode/text/50/403–5d [traducción propia]

(1) […] El director de la Agencia Federal de Investigaciones, o a quien éste designe […] puede solicitar una orden para requerir cualquier cosa tangible (incluidos libros, grabaciones, papeles, documentos y otros elementos), para realizar una investigación destinada a obtener información de Inteligencia extranjera que no concierna a ciudadanos estadunidenses, o para proteger de actividades internacionales terroristas o actividades clandestinas de Inteligencia bajo la condición de que la investigación de una persona de Estados Unidos no afecte las bases de actividades protegidas por la Primera Enmienda.[98]

[…] ninguna persona deberá develar a ninguna otra (con excepción de aquellas necesarias para producir el bien tangible) que la Agencia Federal de Investigaciones ha solicitado u obtenido cosas tangibles bajo esta sección.[99]

1.2.7 Enmienda para proteger América, de 2007

En 2007 se promulgó otra enmienda a la Ley FISA, la cual validó mayores alcances de vigilancia para la comunidad de Inteligencia, con el nombre *de Protect America Act of 2007.* Se encuentra en la sección 1801del título 50 del USC.

Al respecto, cabe recordar que con la adopción de la "FISA *Amendment Act* (FAA), de 2007, "el procurador general y el director nacional de Inteligencia pueden otorgar a la NSA una autorización para la recolección de información global, renovable todos los años, sometida a la aprobación de la FISC. Los agentes ya no tienen que justificar la vigilancia ante la justicia, lo que permite una interceptación masiva."[100] En el acta, esta información se encuentra en la sección dos, en donde se lee: "Secc. 2. Procedimientos adicionales para autorizar ciertas adquisiciones de información de Inteligencia extranjera. La Ley de Inteligencia del extranjero de 1978 […] se enmienda al insertársele […] lo siguiente: Esclarecimiento de la vigilancia

[98] "La Primera Enmienda de la Constitución de Estados Unidos, protege el derecho de libertad de religión y libertad de expresión respecto de la interferencia gubernamental. Prohíbe cualquier ley que establezca una religión nacional que impida el libre ejercicio religioso, reduzca la libertad de expresión, transgreda la libertad de prensa, interfiera con el derecho pacífico de asamblea, o prohíba a los ciudadanos solicitar al gobierno reparación de agravios […]", "First Amendment an Overview", *Legal Information Institute, Cornell Law School*, https://www.law.cornell.edu/wex/first_amendment [traducción propia]

[99] 50 U. S Code SS 1861- *Acces to certain business records for foreign intelligence and international terrorism investigations, U.S Code, Chapter 36, Subchapter I*V, sección 1861, *Legal Information Institute, Cornell Law School*, https://www.law.cornell.edu/uscode/text/50/1861 [traducción propia]

[100] Antoine Lefébure, *El caso Snowden. Así espía Estados Unidos al mundo, op.cit.,* p. 171.

electrónica fuera de Estados Unidos"[101], como también "procedimientos adicionales para autorizar ciertas adquisiciones concernientes a personas localizadas fuera de Estados Unidos"[102]. Esto significa que tanto el director de Inteligencia Nacional como el procurador general pueden autorizar la adquisición de Inteligencia exterior que, se supone, se encuentra fuera de Estados Unidos. "La adquisición contempla la obtención de información de Inteligencia extranjera de o con la asistencia de un proveedor de servicios de comunicación, custodio u otra persona (incluye cualquier oficial, empleado, agente u otra persona especificada por dicho proveedor de servicios, custodio, u otra persona) que tenga acceso a las comunicaciones, ya sea cuando éstas se transmitan o mientras se almacenan, o el equipo que es o puede ser usado para transmitir o almacenar dichas comunicaciones."[103]

Al ser una ley para regular el comportamiento del gobierno en territorio interno, no se encuentra regulada por los órganos judiciales de Estados Unidos. La ley y su tribunal se encuentran en una parte del Código de Estados Unidos para la Guerra y la Defensa Nacional *(U.S Code for War and National Defense)*. En consecuencia, son una ley y un tribunal que responden a tiempos de guerra y tienen como propósito el espionaje para garantizar la Seguridad Nacional, misma que alcanza niveles extraterritoriales.

1.3 Los programas de espionaje

1.3.1 Proyecto Minaret y Operación Shamrock

Desde su nacimiento, la NSA creó programas de espionaje con la complicidad de empresas privadas de las comunicaciones. La Operación Shamrock, "que comenzó en la Segunda Guerra Mundial, buscaba recolectar la mayor parte de los telegramas que entraban o salían de Estados Unidos. En la práctica, la recolección la realizaban de forma directa las empresas de redes de telegrafía: ITT, RCA y Western Union. Luego éstas transmitían a la agencia las copias de todos los telegramas internacionales. La época obligaba a que los microfilmes fueran trasportados en tren desde Nueva York hasta Fort Meade, en Maryland (sede de la NSA), por mensajeros juramentados. Pronto los microfilmes fueron reemplazados por bandas magnéticas mucho más

[101] "Protect America Act of 2007", 121 STAT. 552. PUBLIC LAW 110-55- 110th Congress, https://www.gpo.gov/fdsys/pkg/STATUTE-121/pdf/STATUTE-121-Pg552.pdf [traducción propia]
[102] *Ídem.*
[103] *Ídem.*

pesadas; así, cada mes se entregaban 150, 000 telegramas que eran analizados por los agentes de la NSA con miras a producir informes para la CIA y el FBI".[104]

A lo largo de la "Guerra Fría" y de la invasión de Estados Unidos a Vietnam, los movimientos pacíficos escalaron en Estados Unidos. El presidente Lyndon B. Johnson justificó el espionaje de la época al peligro que el comunismo representaba para la forma de vida estadunidense.

En su artículo de investigación denominado "Documentos secretos de la Guerra Fría revelan el espionaje de la NSA a senadores... junto con Muhammad Ali, Martin Luther King, y un humorista *Washigton Post" (Secret Cold War Documents Reveal NSA Spied on Senators... along with Muhammad Ali, Martin Luther King, and a Washington Post humorist)*", el historiador Matthew M. Aid y William Burr, analista del Archivo de Seguridad Nacional (*National Security Archive*), afirmaron lo siguiente:

> La escalada de la disidencia enojó a Jonson, así como a su sucesor, Richard Nixon. Como fervientes anticomunistas que fueron, se preguntaban si las protestas domésticas estaban relacionadas con poderes extranjeros hostiles, y querían respuestas de la Comunidad de Inteligencia. La CIA respondió con la Operación Chaos, mientras que la NSA trabajó en conjunto con otras agencias gubernamentales para crear listas de vigilancia de críticos a la guerra y así vigilar sus comunicaciones de ultramar. Para 1969 este programa, llamado Minaret, se estableció formalmente.[105]

El proyecto Minaret funcionó como un programa hermano del proyecto Shamrock, "En 1967, a pedido del presidente Johnson y del FBI, la NSA establece una lista llamada de los 'desórdenes civiles' para saber si las organizaciones que luchaban contra la guerra de Vietnam, o las que militaban por los derechos cívicos de los negros, recibían apoyo de gobiernos extranjeros. […] la NSA se dio a la tarea de inspeccionar las interceptaciones telefónicas y telegráficas de Shamrock, cuidando, al mismo tiempo, que los documentos particularmente

[104]Antoine Lefébure, *El caso Snowden. Así espía Estados Unidos al mundo, op. cit.,* p. 120.
[105]Matthew M. Aid, William Burr, "Secret Cold War Documents Reveal NSA Spied on Senators...along with Muhammad Ali, Martin Luther King, and a Washington Post humorist", Investigation, Foreign Policy, 25 de septiembre de 2014, http://foreignpolicy.com/2013/09/25/secret-cold-war-documents-reveal-nsa-spied-on-senators/ [traducción propia]

sensibles o confidenciales se difundieran de manera muy limitada. Se encuentran rastros de colaboración estrecha entre las dos agencias gubernamentales en un mensaje enviado a la NSA […] por el director del FBI, John Edgar Hoover".[106]

En consideración a lo anterior, es evidente que ambos programas servían para espiar a los ciudadanos que no compartían la política exterior de Estados Unidos. Minaret y Shamrock demuestran el complejo sistema de espionaje que funcionó después de la Segunda Guerra Mundial y la cooperación entre agencias de la Comunidad de Inteligencia. Aunque ambos son proyectos para el espionaje doméstico, son los antecesores de Upstream y PRISM, los programas que en la actualidad funcionan para la IC.

El alcance del programa fue tal, que "durante los seis años que duró Minaret, la NSA monitoreó las comunicaciones telefónicas y de cable de ultramar de 1, 650 ciudadanos estadunidenses, la mayoría pacifistas, líderes de movimientos por los derechos civiles y miembros de lo que los dirigentes de la Casa Blanca llamaron extremistas o miembros de organizaciones subversivas".[107]

La NSA se dedicó a la escucha de sus ciudadanos, de aliados y de enemigos. En 1960 quedó constancia de las escuchas de la NSA a causa de las declaraciones de dos de sus criptógrafos, William Hamilton Martin y Bernon F. Mitchell, mismos que confesaron el uso de aviones militares equipados para la escucha de radios y el espionaje a radares, que "dejan detrás de sí una carta en la que denuncian los provocadores vuelos de la NSA y se sublevan contra 'el dinero y los recursos militares movilizados para derrocar a los gobiernos considerados adversarios de Estados Unidos'. (...) En una conferencia de prensa organizada en Moscú por el Kremlin, renuevan sus acusaciones y revelan el espionaje de las comunicaciones de las potencias aliadas. 'Italia, Turquía, Francia, Indonesia', entre otras, son escuchadas por la NSA".[108] Otro ejemplo de cómo funcionó la NSA, es la Operación de Soto, "una campaña marítima de espionaje de las telecomunicaciones de las fuerzas del Viet Minh y del Viet Cong."[109]

Desde entonces hasta ahora, no muchas cosas han cambiado. Por ejemplo, el 30 de

[106]Antoine Lefébure, *El caso Snowden. Así espía Estados Unidos al mundo, op. cit.*, p. 121.
[107]Matthew M. Aid, William Burr, "Secret Cold War Documents Reveal NSA Spied on Senators...along with Muhammad Ali, Martin Luther King, and a Washington Post humorist", *op. cit.*
[108]Antoine Lefébure, *El caso Snowden. Así espía Estados Unidos al mundo, op. cit.,* p. 125.
[109] *Ibíd*., 127.

noviembre de 2015, John Kiriakou[110], quien fue agente de la CIA en contraterrorismo e investigador de alto nivel en el Comité de Relaciones Exteriores del Senado, publicó en el portal de noticias de Internet *Reader Supported News,* que el servicio de correo de los Estados Unidos (USPS, por sus siglas en inglés) espía a los ciudadanos.

John Kiriakou reveló, asimismo, la "recolección sistemática de información de cada correo recibido o enviado, incluidos los nombres y la dirección del emisor y del destinatario, sin una orden judicial o vigilancia institucional, y sin la necesidad de justificar por qué una persona es vigilada."[111]. Kiriakou también escribió que el programa de espionaje del servicio postal espió a 8, 000 objetivos anualmente entre los años 2000, antes de los eventos del 11 de septiembre de 2001, y 2012. Para 2013, la cifra se disparó a 49, 000. El espionaje al correo de las personas se realiza bajo los supuestos de Seguridad Nacional, por lo que para hacerlo no se necesitan órdenes judiciales ni la aprobación de ninguna corte.

En relación con Operación Shamrock y Minaret, su importancia radica en que después de la Segunda Guerra Mundial se estableció una serie de programas para la vigilancia de las comunicaciones, los cuales han evolucionado junto con la tecnología, pero no han cesado de funcionar. "Minaret y su programa hermano, Operación Shamrock, fueron los antecesores del programa doméstico de escuchas ilegales que la administración de George W. Bush aplicó de 2001 a 2004".[112] En la actualidad ya puede conocerse, por documentos desclasificados, el número de "objetivos" que la NSA espió con ambos programas; Matthew M. Aid y William Burr estimaron, en el artículo mencionado, que de 1967 a 1973 la NSA emitió aproximadamente 1, 900 reportes relativos a terrorismo, protección a ejecutivos y la influencia extranjera en grupos que Estados Unidos consideraba subversivos, en particular los agrupaciones con características pacifistas.

Shamrock y Minaret actuaron, así, como programas al interior de Estados Unidos. Sin embargo, le hicieron ver a la Comunidad de Inteligencia la eficiencia del espionaje. "El interés

[110] John Kiriakou pasó veintitrés meses en prisión por denunciar el ilegal programa de tortura de la CIA. Para más información al respecto revisar la liga: http://readersupportednews.org/opinion2/277-75/33772-the-us-postal-service-is-spying-on-us

[111] John Kiriakou, "The US Postal Service Is Spying on Us", Reader Supported News, 30 de noviembre de 2015, http://readersupportednews.org/opinion2/277-75/33772-the-us-postal-service-is-spying-on-us [traducción propia]

[112]Matthew M. Aid, William Burr, "Secret Cold War Documents Reveal NSA Spied on Senators...along with Muhammad Ali, Martin Luther King, and a Washington Post humorist", *op. cit.*

de una estructura tal es que sirve tanto para espiar a los enemigos como a los aliados"[113], también poseen a Echelon, un sistema en el que cuentan con la ayuda de sus aliados para operarlo. "Los estadunidenses tuvieron muy temprano la certeza de que el hecho de disponer de una estructura eficaz de interceptación de las telecomunicaciones constituía una ventaja política y estratégica fundamental".[114]

1.3.2 El sistema UKUSA

1.3.2.1 *Five Eyes* y SIGINT

En mayo de 1976, la revista inglesa *Time Out* publicó, en la edición del 21 al 27 de mayo, el artículo "Los fisgones" *(The Eavesdroppers).* Escrito por Duncan Campbell y Mark Hosenball, causó revuelo al exhibir la complicidad de los gobiernos estadunidense e inglés en la creación de un aparato de espionaje electrónico de alcance mundial, hasta entonces sin precedentes.

La pieza periodística reveló la existencia de UKUSA, tratado secreto firmado en 1947 por Estados Unidos y Gran Bretaña, cuyo propósito fue: "mejorar la eficacia de sus intercambios para la interceptación de las comunicaciones dentro del bloque soviético."[115] En 1955 se adhirieron al tratado Canadá, Australia y Nueva Zelanda, formándose un bloque de cinco países. "Estas cinco naciones de habla inglesa se dividieron, por regiones, la vigilancia mundial de las comunicaciones. La agencia de señales de Inteligencia de cada país, SIGINT, por sus siglas en inglés, está autorizada para el monitoreo de las comunicaciones de la región asignada".[116]

Estas agencias son las siguientes: la Agencia de Seguridad en Estados Unidos, NSA; el Cuartel General de Comunicaciones del Gobierno, GCHQ, por sus siglas en inglés, de Gran Bretaña; la Oficina de Directores de las Señales de Defensa, DSD, por sus siglas en inglés, en Australia; la Oficina de Seguridad de las Comunicaciones del Gobierno, GCSB, por sus siglas en inglés, de Nueva Zelanda, y el Complejo de Seguridad de las Comunicaciones, CSE, por sus siglas en inglés, de Canadá.

En la actualidad el tratado continúa vigente. Y los mismos países continúan integrándolo.

---

[113]Antoine Lefébure, *El caso Snowden. Así espía Estados Unidos al mundo, op. cit.,* pp. 122 y 123.
[114] *Ídem.*
[115]Antoine Lefébure, *El caso Snowden. Así espía Estados Unidos al mundo*, *op. cit.,* p. 182.
[116]Duncan Campbell y Mark Hosenball, "The eavesdroppers", Time Out, No. 21-27 de mayo de 1976, http://www.duncancampbell.org/menu/journalism/timeout/Eavesdroppers.pdf , [traducción propia]

"Es el mismo tratado entre Gran Bretaña, Estados Unidos, Australia, Nueva Zelanda y Canadá el que aún gobierna el intercambio de las señales de Inteligencia comúnmente conocido como '*5-Eyes*'".[117] La cooperación entre estos países subsiste y es más estrecha a causa de la tecnología. "La recolección de 'Inteligencia' se ha desarrollado más con las interceptaciones a las comunicaciones digitales".[118] "Sabemos, por los documentos filtrados por […] Edward Snowden, que la NSA ha sido capaz de retener grandes cantidades de datos provenientes de Inglaterra y de los otros países de *5-Eye*s, permitiendo que se recolecte información de ciudadanos comunes".[119]

1.3.2.2 Diccionarios Echelon

La red Echelon está constituida por las "estaciones terrestres de escucha de las telecomunicaciones satelitales cuyo nombre oficial es Fornsat."[120] "Echelon se asocia con la 'red global' de computadoras que de manera automática hurgan, por medio de palabras clave programadas, entre los millones de mensajes interceptados de fax, télex y correos electrónicos. Los procesadores de dicha red se conocen como Diccionarios Echelon. Echelon conecta a todas las computadoras de esta red y permite que las estaciones funcionen como elementos distribuidos en un sistema integral. Un Diccionario Echelon de una estación contiene, además de las palabras clave de las estaciones, listas de las cinco agencias que pertenecen al sistema UKUSA".[121] La existencia de la red Echelon no se puede explicar sin el tratado UKUSA, que fue el que le dio su origen.

Las agencias pertenecientes a UKUSA son anglosajonas y de países que ganaron la Segunda Guerra Mundial. El sistema Echelon está integrado por las bases de espionaje pertenecientes a los *Five-Eyes*. En 1988, el periodista escocés Duncan Campbell advirtió en su artículo: "Alguien está escuchando, lo tienen intervenido" *(Somebody's listening. They've got it taped),* que la alianza anglo-estadunidense expandiría el complejo millonario de la vigilancia electrónica global. El artículo especifica, con apego a información del Congreso de Estados

[117]Paul Farrell, "History of 5-Eyes-explainer", The Guardian, International edition, Lunes 2 de diciembre de 2013, disponible en http://www.theguardian.com/world/2013/dec/02/history-of-5-eyes-explainer, [traducción propia]
[118] *Ídem.*
[119]*Ídem.*
[120]Antoine Lefébure, *El caso Snowden. Así espía Estados Unidos al mundo, op. cit.,* p.160.
[121]s/a, "Echelon", FAS*,* fas.org/irp/program/process/echelon.htm

Unidos, que "el sistema de vigilancia habilitará a las agencias para monitorear y analizar las comunicaciones de civiles en el siglo XXI".[122] La red Echelon "constituye, así, el último avatar tecnológico de la alianza UKUSA"[123] del siglo XX.

El objetivo de la red Echelon es recolectar información con fines de Inteligencia. Empero, según el actual discurso oficial su finalidad es la lucha contra el terrorismo; por esta razón es importante tener en consideración la opinión del periodista Nicky Hager, quien durante años investigó la red Echelon: "cuando se dice que la Inteligencia estadunidense está dirigida contra el terrorismo, es porque se intenta mantener al público callado y feliz. En realidad, la Inteligencia estadunidense espía las transacciones comerciales y a las organizaciones internacionales, incluso las europeas, sus políticas y preferencias, a las agencias de seguridad y las organizaciones no gubernamentales. Su objetivo es obtener más poder político".[124]

El sistema Echelon controlaba, en 2013, el "90 por ciento de las comunicaciones mundiales. Además, dispone de por lo menos 120 estaciones fijas y satélites geoestacionarios".[125] Las estaciones de la red Echelon varían conforme a la fuente, no obstante, se pueden encontrar consistencias. Duncan Campbell le facilitó a Antoine Lefébure la lista inédita de las estaciones de la red Echelon actualizadas hasta 2013.

Lugar	País	Nombre en código
Yakima	Estados Unidos	Jacknife
Sugar Grove	Estados Unidos	Timberline
Sabana Seca	Puerto Rico	Coralina
Harrogate (Menwith Hill)	Reino Unido	Moonpenny
Misawa	Japón	Ladylove
Bad Aibling	Alemania	Garlick

[122]Duncan Campbell, "Somebody's listening. They've got it taped", The New Statesman Society, 12 de agosto de 1988.
[123]Antoine Lefébure, *El caso Snowden. Así espía Estados Unidos al mundo,* Le Monde diplomatique, "el Dipló" y Capital Intelectual, Buenos Aires, 2014, p. 188.
[124]Echelon: el gigante de espionaje de EE.UU. que no estaba dormido, disponible en: https://actualidad.rt.com/actualidad/view/102742-echelon-eeuu-espionaje-nsa-guerra-fria
[125]Echelon: el gigante de espionaje de EE.UU. que no estaba dormido, disponible en: https://actualidad.rt.com/actualidad/view/102742-echelon-eeuu-espionaje-nsa-guerra-fria

Fuente: Antoine Lefébure, *El caso Snowden. Así espía Estados Unidos al mundo,* p. 160.

Finalmente, la red Echelon dejó de ser un secreto. Su funcionamiento fue ampliamente investigado por el parlamento de la Unión Europea hasta conocer su función. La preocupación que mostró el reporte de dicho parlamento radica en que "el sistema de espionaje se usa para reunir información industrial estratégica y se le pasa a los rivales británicos y estadunidenses".[126] Más aún, el mayor temor obedece a la posibilidad de que Echelon se convierta en una policía secreta cibernética. La palabra cibernético, la cual en la actualidad se utiliza para designar lo concerniente a la realidad virtual, proviene del griego y significa: "El arte de gobernar una nave".[127]

Fuente: "Echelon", Duncan Campbell[128]

[126]Jane Perrone, "The Echelon spy network", The Guardian, International edition, 29 de mayo de 2001, http://www.theguardian.com/world/2001/may/29/qanda.janeperrone
[127] *Diccionario de la Lengua Española,* Real Academia Española, en línea, entrada: "Cibernético".
[128] Duncan Campbell, "Echelon"; Duncan Campbell.org, Investigative journalist & forensic expert, http://www.duncancampbell.org/content/echelon

1.3.3 Las nuevas dimensiones del espionaje

Después de los atentados del 11 de septiembre de 2001, el gobierno estadunidense lanzó el discurso para proteger a Estados Unidos de los ataques de los chicos malos *(bad guys)*, y lanzó su guerra contra el terror *(War on Terror)*. No se pretende desarrollar, aquí, un análisis discursivo del significado de "chico malo", o del terror. Conviene, no obstante, citar al respecto al sociólogo estadunidense Morris Berman en su libro *Edad Oscura Americana. La fase final del imperio:*

> La religión también aparece en la actual tendencia americana de explicar los eventos mundiales (en particular, los ataques terroristas) como parte de un conflicto cósmico entre el bien y el mal, en lugar de comprenderlos en términos de procesos políticos. Esto difícilmente se limita a la Casa Blanca. El maniqueísmo rige en Estados Unidos. De acuerdo con una encuesta realizada por la revista *Time* –¿de verdad puede esto ser cierto?– el cincuenta y nueve por ciento de los americanos creen que las profecías apocalípticas de Juan en el *Libro de las Revelaciones* se cumplirán, y casi todos ellos creen que los fieles serán llevados al cielo en el 'Éxtasis' (Tratado de Tesalonicenses). De acuerdo con el *Libro de las Revelaciones,* Dios castigará a los no creyentes con varias plagas, tras lo cual Cristo regresa a la Tierra –con una espada en la boca– para la lucha final entre el Bien y el Mal (la batalla de Armagedón).[129]

Este discurso, en términos de Inteligencia se tradujo y conoció como el programa del presidente: Stellarwind (Viento Estelar) .[130]

1.3.3.1 Stellarwind

Stellarwind fue el nombre, en código, de la operación de vigilancia, escuchas telefónicas y recopilación de metadata[131] que autorizó George W. Bush como medida para combatir el terrorismo. Stellarwind fue clasificado como información secreta del más alto nivel para desclasificarse en no menos de veinticinco años. El director de la NSA era Keith B. Alexander.

[129] Morris Berman, *Edad Oscura Americana. La fase final del imperio*, *op. cit*., p. 27.
[130] *Stellarwin,* en español se podría traducir como viento estelar, o incluso, como viento soberbio.
[131] Metadata, ver glosario.

El general Keith Alexander "se jactó, ante la Comisión Judicial del Senado, de emplear a 960 catedráticos, 4, 000 ingenieros en informática y más de 1, 000 matemáticos (la NSA es el primer empleador de matemáticos en Estados Unidos)"[132], aunque no hay ninguna certeza en tal sentido, pues el número de empleados, en ese entonces como ahora, se desconoce. Por ley está prohibido develar el número real. Las estimaciones oscilan entre 30, 000 y 40, 000, pero la cifra real se enmarca como información clasificada.

A continuación se reproduce la portada del documento *(U//FOUO) Stellarwind Classification Guide (2-400)*[133], utilizado para entender en qué consistió la operación. Aunque el documento es tan sólo una guía de la clasificación de los distintos elementos del programa, es valiosísimo porque nos permite vislumbrar sus alcances. Las primeras informaciones del programa, aún sin conocerse el nombre del mismo, salieron a la luz pública en diciembre de 2005. El 17 de diciembre de ese año, el presidente hizo una declaración en la que seleccionó algunos aspectos del programa para hacerlos del conocimiento público, mientras otros permanecieron en calidad de clasificados.

TOP SECRET//SI//ORCON/NOFORN

NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE

(U//FOUO) STELLARWIND Classification Guide
(2-400)

Effective Date: 21 January 2009

Classified by: Keith B. Alexander,
Lieutenant General, USA
Director, NSA

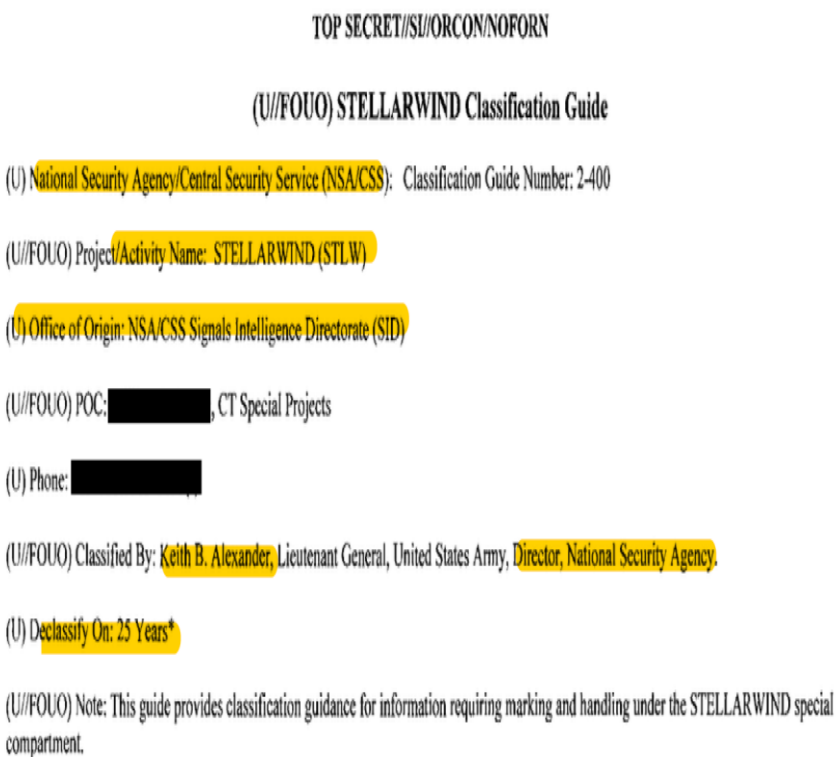
Reason(s) for Classification:
E.O. 12598, 1.4(c)

Declassify on: 25 Years*

Endorsed by: Joseph Brand
Associate Director, CIPR

Fuente: *The New York Times*

[132]Antoine Lefébure, *El caso Snowden. Así espía Estados Unidos al mundo, op.cit.,* p. 156.
[133] Charlie Savage, "Classification Guide for Stellarwid Program", *The New York Times,* 11 de marzo de 2014, https://www.nytimes.com/interactive/2014/03/12/us/stellarwind-guidance-doc.html
*(U//FOUO) Stellarwind Classification Guide (2-400), se puede descargar en su totalidad de la página del *NYT.*



TOP SECRET//SI//ORCON/NOFORN

(U//FOUO) STELLARWIND Classification Guide

(U) National Security Agency/Central Security Service (NSA/CSS): Classification Guide Number: 2-400

(U//FOUO) Project/Activity Name: STELLARWIND (STLW)

(U) Office of Origin: NSA/CSS Signals Intelligence Directorate (SID)

(U//FOUO) POC: [redacted], CT Special Projects

(U) Phone: [redacted]

(U//FOUO) Classified By: Keith B. Alexander, Lieutenant General, United States Army, Director, National Security Agency.

(U) Declassify On: 25 Years*

(U//FOUO) Note: This guide provides classification guidance for information requiring marking and handling under the STELLARWIND special compartment.

Fuente: *The New York Times*

Después, en 2007, la Ley FISA fue objeto de la enmienda *Protect America Act*, que vimos en el apartado anterior. Con ésta se volvían legítimas las prácticas que fueron controversiales en 2005. El documento que se encontró y mostró corresponde a 2009. En ese entonces, ya aprobadas las reformas de 2007, Stellarwind seguía en funciones.

Del documento se destaca lo siguiente:

Información no clasificada.

Esta información no es clasificada, se conoció en la declaración pública presidencial. 17 de diciembre de 2005, en el Salón Roosevelt de la Casa Blanca.

- […] la NSA contaba con autoridad del presidente para intervenir las comunicaciones internacionales de personas con conocidos vínculos con Al Qaeda y organizaciones terroristas relacionadas.
- Las actividades autorizadas bajo autoridad presidencial eran revisadas cada cuarenta y cinco días.
- El programa autorizado por el presidente fue reautorizado más de treinta veces. Más de una docena de veces se les informó a líderes del Congreso de las autorizaciones

presidenciales y de las actividades desarrolladas.

- La autorización presidencial le permitió a la NSA interceptar los contenidos de las comunicaciones en las que parte de la comunicación se encontraba fuera de Estados Unidos. No clasificado. Declaración pública del fiscal general Alberto González, 19 de diciembre de 2005, respecto de la vigilancia de la NSA.
- La identidad de los abogados del Departamento de Justicia que representan o han representado a la NSA, o han sido identificados públicamente como autorizados para TSP.

Información clasificada como SECRET//NOFORN por veinticinco años.

- El hecho de que Stellarwind es un programa antiterrorista.
- El hecho de que la presidencia autorizó TSP dentro de la NSA es un componente de Stellarwind. Este programa también puede encontrarse como TSP, COMPARTMENTED.

Información clasificada como TOP SECRET//NOFORN por veinticinco años.

- La lista de todos los individuos con acceso a Stellarwind o a los datos producidos por el programa.
- Nombres de personal de las ramas ejecutiva, legislativa o judicial autorizado para STLW que no han sido públicamente identificados por la rama ejecutiva.
- La información de contraterrorismo producida por STLW utilizada para evaluar la cantidad o el valor de la colección de Stellarwind en productos/pistas sin referencia a los objetivos, métodos o técnicas.
- Información que revele el alcance de recolección de Stellarwind a varios métodos de comunicación que incluyen voz, redes de data, telefax, etcétera. Incluye la información recopilada por distinto métodos bajo STLW y subsecuentemente autorizada bajo FISA (17 enero de 2007) o PAA (5 de agosto de 2007).
- El alcance de la colección de Stellarwind y el número de solicitudes para obtener información.
- La información que revele la relación operacional entre Stellarwind, FISA y la recolección bajo FAA y PAA.

- Las listas creadas bajo Stellarwind o los reportes que detallen la totalidad de técnicas específicas bajo el programa es información confidencial hasta por veinticinco años.
- Información que revele el alcance de las operaciones bajo la autorización presidencial como técnicas de recolección, objetivos u otros detalles operativos que no fueron hechos públicos por el presidente.
- Es pública la colaboración de la CIA en el programa STLW y que la NSA proveyó la información recolectada bajo el programa del presidente a la CIA; sin embargo, es información clasificada hasta por 25 años el hecho de que la CIA jugó un rol operacional en el programa y los detalles de éste.
- Bajo el hecho de las colaboración del FBI en el programa STLW, es público que la NSA proveyó la información recolectada bajo el programa del presidente al FBI, sin embargo, es información clasificada hasta por 25 años el hecho de que el FBI jugó un rol operacional en el programa y los detalles de ese programa.
- Información de los proveedores de comunicaciones. No está clasificado el hecho de que proveedores de servicios de comunicación proveyeron asistencia en materia de Seguridad Nacional. Sin embargo, con base en la reforma a la Ley FISA de 1978 y las enmiendas de 2007, es clasificada como información TOP SECRET//NOFORN hasta por veinticinco años la información que revele las relaciones con y las identidades de los proveedores de telecomunicaciones estadunidenses bajo las autoridades de Stellarwind.
- Información que revele la localización o las instalaciones que proveen acceso o recolección a Stellarwind.
- El flujo de información creada para apoyar la recolección de datos de Stellarwind sin revelar detalles de la autorización presidencial.
- Descripciones, diagramas, esquemas u otra documentación técnica que identifique los métodos específicos o técnicas y aparatos de SIGINT usados para seleccionar, filtrar o procesar comunicaciones sin referencia a la autorización y creación del programa.
- El análisis de metadatos y el proceso de objetivos, técnicas y resultados de Stellarwind, sin detalles específicos de la autorización o puntos de acceso de los que se recolecta la

información.

- Metadatos de la red de Inteligencia digital recolectada bajo autorización presidencial antes del 17 de julio de 2004.
- La metadata adquirida bajo el Reconocimiento de Números Marcados, DNR, por sus siglas en inglés, bajo la autorización presidencial de antes de mayo de 2006 y el archivo de metadata consecuente de dicha recolección.
- Los reportes de metadata del DNI, incluyendo toda la metadata derivada de la autorización especial de la corte FISA marcada como Stellarwind.
- Los reportes de metadata del DNR, incluyendo toda la metadata derivada de la autorización especial de la corte FISA marcada como Stellarwind.

1.3.3.1.1 PRISM y Upstream

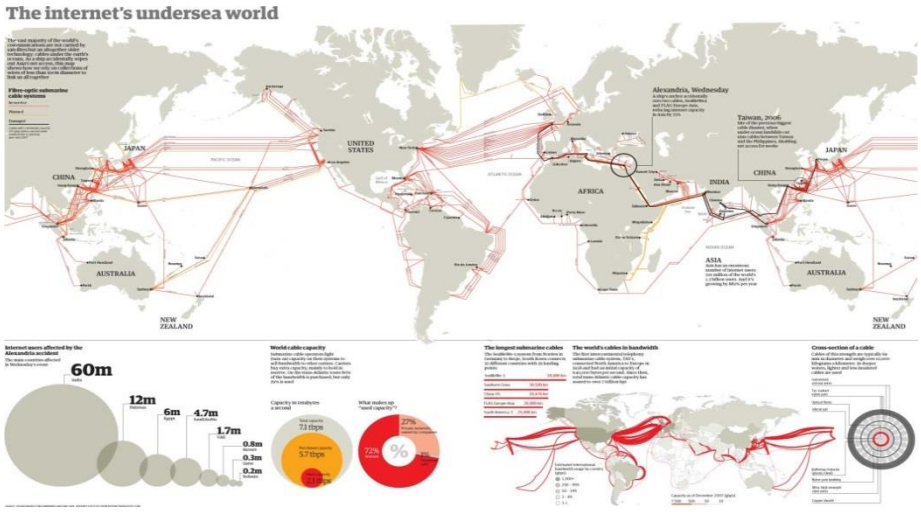
Como consecuencia de las filtraciones de Edward Snowden, se hizo de conocimiento general la existencia de dos programas enmarcados en la respuesta a los atentados del 11 de septiembre y de la guerra contra el terror. Estos programas son PRISM y Upstream. Cabe al respecto subrayar que PRISM no puede comprenderse sin la existencia de Upstream, porque así como Shamrock y Minaret operaban en conjunto, aquellos dos programas trabajan en conjunto para obtener la mayor cantidad de información acerca de los objetivos que espían. Podemos por consiguiente suponer que ambos son parte esencial de la operación Stellarwind.

En la diapositiva filtrada por el exanalista de la NSA, Edward Snowden, denominada *FAA702 Operations. Two types of Collection*, la oficina estadunidense *Special Source Operation* "recomienda" hacer uso de ambos programas para recolectar la información digital. Upstream se utiliza para obtener la información de las comunicaciones contenida en los cables de fibra óptica mientras los datos pasan por ellos. Y PRISM para la recolección de datos que proviene de los servidores estadunidenses[134]: Microsoft, Yahoo, Google, Facebook, PalTalk, Skype, YouTube y Apple. Los datos anteriores parecieran no tener mayor relevancia si no se considera la estructura de los cables submarinos de fibra óptica. La capacidad de Estados Unidos para controlar los flujos de información por internet es la mayor en el mundo; "el 80

[134] s/a, "NSA slides explain the PRISM data-collection program", *The Washington Post,* abril de 2013 http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/

por ciento del tráfico mundial de internet proviene de Estados Unidos, (es decir), la NSA tiene sobre éste un control casi absoluto."[135]

TeleGeography, firma consultora de los mercados de las telecomunicaciones, elabora anualmente un mapeo de los cables de fibra óptica. En la información filtrada por Edward Snowden se muestra a esta fuente como referencia del gobierno de Estados Unidos. El mapa del cableo exhibe todas las conexiones de la infraestructura de fibra óptica y cómo el tráfico de información de internet irremediablemente sale, regresa o pasa por Estados Unidos.



Fuente: *The Guardian*[136]

En el artículo de *The Washington* intititulado "Las diapositivas de la NSA explican el programa de recolección de información PRISM" *(NSA slides explain the PRISM data-collection program)*, se confirma que el "ultrasecreto programa PRISM permite a la Comunidad de Inteligencia beneficiarse del acceso que tienen nueve compañías de internet, ya mencionadas, a gran cantidad de información digital, que incluye correos electrónicos y datos almacenados de objetivos extranjeros que operan fuera de Estados Unidos."[137]

El artículo también menciona al FBI como la dependencia especializada en revisar los contenidos que le brinda PRISM. La Unidad de Vigilancia de las Comunicaciones Electrónicas (FBI-ECSU, por sus siglas en inglés), transfiere la información recolectada a otros "clientes", como la CIA o la NSA.

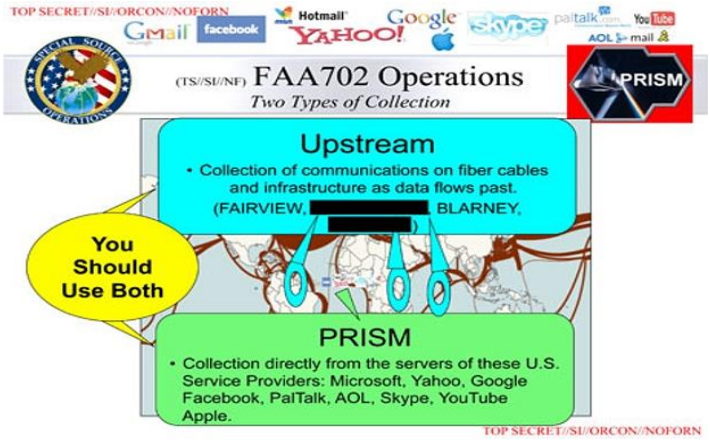
---

[135] Antoine Lefébure, *El caso Snowden. Así espía Estados Unidos al mundo, op. cit.,* p. 161.
[136] s/a, "The Internet´s undersea world", *The Guardian,* 1 de febrero de 2008, http://image.guardian.co.uk/sys-images/Technology/Pix/pictures/2008/02/01/SeaCableHi.jpg
[137] s/a, "NSA slides explain the PRISM data-collection program", The Washington Post, abril de 2013 http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/

En otra de las diapositivas filtradas por Edward Snowden, denominada *PRISM Case Notations*, también publicada por *The Washington Post,* se enumera a los nueve proveedores de PRISM y se especifica a qué clase de información puede tenerse acceso. La diapositiva presenta los siguientes rubros: a) las búsquedas de internet de los usuarios; b) pláticas electrónicas o *chats*; c) acceso en tiempo real a los correos electrónicos, ya sea al iniciar sesión o al enviar un correo; d) notificaciones en tiempo real al iniciar sesión en un chat o al terminar la sesión; e) acceso a correos electrónicos; f) acceso a VolP[138]; g) foros en la Web; h) mensajes OSN; i) información de suscripciones OSN [*Open Storage Networking*] y j) videos. Con esta información podemos tener una buena idea de la cantidad de datos que maneja el programa PRISM. En otra diapositiva, ésta fechada el 5 de abril de 2013, titulada *REPRISMFISA TIPS,* puede constatarse la presencia de 117, 675 objetivos. Y éstos tan sólo en la base de datos de contraterrorismo.

PRISM comenzó a recolectar datos desde 2007, año en el que Microsoft y Apple se incorporaron al programa, hasta la inclusión de su último proveedor en octubre de 2012. Así, Yahoo entró al programa en 2008; Google, Facebook y PalTalk en 2009; YouTube en 2010, y Skype y AOL en 2011.[139] El Programa PRISM tiene un costo anual de 20 millones de dólares.[140]

A continuación se reproduce la diapositiva original emitida por la oficina de *Special Source Operations* y filtrada por E. Snowden, en la que se "recomienda" utilizar ambos programas.



[138] VolP es el lenguaje de comunicación electrónica en el que se realizan llamadas de voz a través del Internet.
[139] s/a, "Dates When PRISM Collection Began For Each Provider", The Washington Post, http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/
[140] *Ídem.*

Además de los programas de espionaje en los que se utilizan la tecnología y las redes de comunicación electrónica, surgió un nuevo aspecto del espionaje: el espionaje electrónico, espionaje cibernético o ciberespionaje. Éste dio lugar a un nuevo lugar de disputa en el que también se libran acciones bélicas o ciberguerras. Para cerrar el capítulo, basta precisar que "el ciberespionaje es el ingreso no autorizado por parte de un Estado-nación en las redes, ordenadores y bases de datos de otro Estado-nación con el propósito de copiar y robar información delicada."[141]

[141]Richard A. Clarke, Robert K. Knake, *Guerra en la red. Los nuevos campos de batalla,* Ariel, Barcelona, 2011, p. 362.

2

Ciberguerra estadunidense y *Silicon Valley*

> "−Los ataques cibernéticos más elegantes, se parecen en cantidad, a los fraudes bancarios−, me dijo en 2011, uno de los primeros arquitectos de *Olympic Games*, mientras comenzaba a hurgar en la manera en que Washington hacía uso de una nueva tecnología, las armas cibernéticas ofensivas. En éstas, gasta miles de millones de dólares cada año y se rehúsa categóricamente a hablar de ello.
> −Cuando mejor funcionan es cuando la víctima no sabe que se le está robando−"[142]

El objetivo de este capítulo es analizar si existe o no una guerra cibernética y, si ésta sostiene relación con las empresas de las tecnológicas de la comunicación.

Para este propósito, se presentan tres Estrategias de Seguridad Nacional, armas cibernéticas, el concepto de lo que podríamos caracterizar como guerra cibernética o ciberguerra, además del impacto de la iniciativa privada.

A mediados de la última década del siglo XX, el geopolítico y asesor del presidente Jimmy Carter, Zbigniew Brzezinski, en su libro *El gran tablero mundial. La supremacía estadunidense y sus imperativos geoestratégicos*, publicó que:

> […] el sistema global estadunidense pone un énfasis en la técnica de cooptación […] mucho mayor que el que ponían los viejos sistemas imperiales. Asimismo, se basa en gran medida en el ejercicio indirecto de la influencia sobre las élites extranjeras dependientes, mientras que obtiene grandes beneficios a partir del atractivo que ejercen sus principios democráticos y sus instituciones. Todo lo anterior se refuerza con el impacto masivo pero intangible de la dominación estadunidense sobre las comunicaciones globales, las diversiones populares y la cultura de masas y por la influencia potencialmente muy tangible de la tecnología de punta estadunidense y de su

[142] David E. Sanger, "Chapter 8, Olympic Games", *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power*, Nueva York, Random House, 2012, e-book, p. 4 de 42. [traducción propia]

alcance militar global.[143]

Como se infiere en la cita anterior, las comunicaciones y la tecnología representan un factor de dominación que determina la política exterior estadunidense y se relaciona con el alcance militar, sus imperativos geoestratégicos y su poder de cooptación. Muestra de ello es la Red Echelon. Como se explicó en el primer capítulo, esta red es un ejemplo que abarca tanto el poder de cooptación de las naciones aliadas, el alcance geopolítico de las bases Echelon que tienen un enfoque militar y el uso que se hace de las comunicaciones y la tecnología.

Las nuevas tecnologías, además de servir para programas de espionaje en un sentido técnico, se han posicionado como parte fundamental de la estructura de Seguridad Nacional y su expresión en la Comunidad de Inteligencia. Esto se observa en el desarrollo de estrategias defensivas, ofensivas y el uso de armas cibernéticas.

2.1 Las Estrategias de Seguridad Nacional

La Estrategia de Seguridad Nacional de Estados Unidos, es un reporte que contiene las acciones y decisiones óptimas de seguridad que intentará llevar a cabo el gobierno en turno. Ésta, es emitida por la oficina de la Casa Blanca y con posterioridad se envía al Congreso. Para el presente estudio se abarcan las Estrategias de Seguridad Nacional publicadas durante los gobiernos de George W. Bush y Barack H. Obama.

2.1.1 Estrategia de Seguridad Nacional de Estados Unidos, septiembre 2002

Siendo presidente de Estados Unidos George W. Bush, la Casa Blanca publicó su Estrategia de Seguridad Nacional de Estados Unidos, septiembre de 2002.[144] En este documento, firmado por el presidente en aquel entonces, se comunicó que "Estados Unidos extenderá la paz al promover las sociedades abiertas y libres en todos los continentes".[145]

Aunque en este informe aún no se menciona al espacio cibernético y la seguridad cibernética; ya aparecen los precedentes para incluir estos aspectos en los informes posteriores.

[143] Zbigniew Brzezinski, "Capítulo 1. Una nueva clase de hegemonía", *El gran tablero mundial. La supremacía estadunidense y sus imperativos geoestratégicos*, s/c, *Paidós,* s/año, p. 34.
[144] En inglés: *The National Security Strategy of the United States of America September 2002*
[145] George W. Bush, *The National Security Strategy of the United States of America September 2002,* https://www.state.gov/documents/organization/63562.pdf, p. 3. [traducción propia]

Estados Unidos equipara la definición de sociedad abierta a la sociedad estadunidense y advierte peligros: "los terroristas están organizados para penetrar en las sociedades abiertas y voltear el poder de las tecnologías modernas contra nosotros";[146] por otro lado, aparecen los conceptos de guerra preventiva y alianza de la voluntad (*Coalition of the willing)*.

En la Estrategia de Seguridad Nacional, se explica el concepto de alianza de la voluntad como herramienta de cooperación internacional. "Las coaliciones de la voluntad pueden expandir la fuerza de estas instituciones permanentes [la Organización de Naciones Unidas, la Organización del Atlántico Norte, la Organización Mundial de Comercio y la Organización de Estados Americanos]. En todos los casos, las obligaciones de las organizaciones internacionales se deben tomar con seriedad."[147] Recordemos que aunque se habla de institucionalidad internacional, se trata de la estrategia a seguir por parte de Estados Unidos para preservar la Seguridad Nacional, misma que entiende además de la defensa del territorio y los intereses nacionales, como las relaciones exteriores para obtener beneficios.

2.1.2 Estrategia de Seguridad Nacional de Estados Unidos, mayo de 2010

En la Estrategia de Seguridad Nacional de Estados Unidos de mayo de 2010[148] firmada por el expresidente Barack Obama, existe ya un apartado dedicado a la seguridad del espacio cibernético.

El Departamento de Defensa entiende al espacio cibernético como "el dominio global dentro del ambiente de la información que consiste en la infraestructura de información tecnológica de la red interdependiente y la información residente, incluyendo Internet; redes de telecomunicaciones, sistemas de cómputo, procesadores y los controladores integrados".[149]

Por seguridad, el Departamento de Defensa cuenta con tres definiciones, "1. Las medidas o actividades tomadas por una unidad o instalación militar para protegerse de todos los actos que puedan perjudicar su efectividad. 2. La condición que resulta del establecimiento y mantenimiento de medidas de protección que aseguren el estado de inviolabilidad por actos o influencias hostiles; y 3. En lo que respecta a materia clasificada, la condición que previene a

[146] *Ídem.*
[147] *Ibíd*., p. 5.
[148] Barack H. Obama*, The National Security Strategy of the United States of America May,* www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf , 60 pp. [traducción propia]
[149] *Dod Dictionary of Military and Associated Terms, as of August 2017*, entrada: Cyberspace, p. 58. [traducción propia]

personas no autorizadas de tener acceso a información oficial que está salvaguardada en interés de la Seguridad Nacional".[150]

Por lo previamente dicho, una primera aproximación a la seguridad del espacio cibernético sería: 1.las actividades militares que aseguren el correcto funcionamiento de la infraestructura que en su conjunto forma al espacio cibernético y 2. La situación que resulta de las medidas de protección para que este ámbito sea inviolable.

Las definiciones anteriores se precisaron a causa de que es en esta Estrategia de Seguridad Nacional donde se menciona por primera vez al espacio cibernético como punto estratégico a proteger. Además, en ésta, se establece que para asegurar la capacidad nacional se necesita de estrategias en defensa, diplomacia, economía, desarrollo, seguridad del hogar, Inteligencia, comunicaciones estratégicas, la población y el sector privado.[151] Respecto a la estrategia en Inteligencia se establece que

> La seguridad y prosperidad de Estados Unidos depende de la calidad de Inteligencia que recolectamos; así como la capacidad para analizarla, la habilidad para evaluar y compartir información de manera oportuna y la habilidad para contrarrestar las amenazas a la misma. Todo esto es cierto y funciona para la Inteligencia estratégica que informa para la toma de decisiones del ejecutivo así como a la Inteligencia que apoya la seguridad del hogar, estatal, local y a gobiernos tribales, a nuestras tropas y las misiones nacionales críticas. Buscamos una mejor integración de la Comunidad de Inteligencia mientras aumentamos las capacidades de los miembros de la misma. Estamos fortaleciendo nuestras asociaciones con servicios de Inteligencia extranjera y nuestros vínculos con nuestros aliados más cercanos. Continuamos invirtiendo en los hombres y mujeres que forman la Comunidad de Inteligencia.[152]

En lo que respecta a las comunicaciones estratégicas; sin tapujos el informe dice que "con el apoyo de todos nuestros esfuerzos, las comunicaciones estratégicas efectivas son esenciales

[150] *Dod Dictionary of Military and Associated Terms, as of August 2017*, entrada: Security, p. 206. [traducción propia]
[151] Barack H. Obama*, The National Security Strategy of the United States of America May, op. cit.,* pp. 15 y 16. [traducción propia]
[152] *Ídem.*

para mantener la legitimidad global y apoyar nuestros objetivos políticos. (…) Debemos incluir una amplia gama de métodos para la comunicación del público extranjero incluyendo los nuevos medios de comunicación masiva".[153]

En la sección tres del mismo informe titulada "Obteniendo nuestros intereses (*Advancing our interest)*", se encuentra el apartado dedicado a la seguridad del espacio cibernético. Se dice que "las amenazas a la seguridad cibernética representan una de las más graves amenazas a la Seguridad Nacional, el bienestar público, y a los retos económicos que enfrentamos como nación"[154]. En el mismo apartado continúa, "las amenazas que enfrentamos abarcan desde hackers criminales hasta grupos de crimen organizado, redes de terroristas hasta Estados-nación avanzados. Defendernos de las amenazas a nuestra seguridad, prosperidad, y privacidad requiere de redes que sean seguras, que tengan nuestra confianza y que sean resilientes."[155]

El documento establece que para lograr defenderse de todas las amenazas contra la Seguridad Nacional cibernética hay dos caminos que deben tomarse: uno, invertir en las personas y en la tecnología, y dos, fortalecer las relaciones con empresas privadas. Argumentan que

> Ni el gobierno, ni el sector privado, ni los ciudadanos, pueden lograr estos retos solos, necesitamos trabajar juntos. También se necesita fortalecer las relaciones internacionales para desarrollar normas de conducta para el espacio cibernético, leyes para el crimen cibernético, prevención de uso de data, protección y privacidad; así como enfoques para la defensa de las redes y para la respuesta a los ataques cibernéticos. Trabajaremos juntos con todos los jugadores clave, incluyendo todos los niveles gubernamentales, y el sector privado nacional e internacional, para investigar la intrusión cibernética y asegurar que haya una respuesta organizada y unificada frente a futuros incidentes cibernéticos.[156]

[153] Ibíd., p. 16.
[154] Barack H. Obama*, The National Security Strategy of the United States of America May, op. cit.,* p. 27. [traducción propia]
[155] *Ídem.*
[156] *Ídem.*

2.1.3 Estrategia de Seguridad Nacional de Estados Unidos, febrero de 2015

En la Estrategia de Seguridad Nacional de Estados Unidos, febrero de 2015[157], y la última en ser publicada; pese a que no hay, como en la de 2010, una sección dedicada a la seguridad cibernética, sí se menciona a ésta en la presentación introductoria firmada por Barack H. Obama.

En este documento, Obama argumenta que Estados Unidos es el país que traza el camino para la ciencia, la tecnología y la innovación en la economía global. Puntualiza que el poder militar de Estados Unidos tiene un alcance tecnológico y geoestratégico sin rivalidad en la historia humana; sin embargo, recalca que se enfrentan serias amenazas a la Seguridad Nacional, "el violento extremismo y la envolvente amenaza terrorista incrementan un persistente riesgo de ataque a Estados Unidos y nuestros aliados. La escalada de desafíos a la seguridad cibernética, las agresiones de Rusia, los impactos del cambio climático, las enfermedades infecciosas, todo esto aumenta las ansiedades acerca de la seguridad global. […] Estados Unidos tiene la capacidad única de movilizar y guiar a la comunidad internacional para enfrentarlas".[158]

Barack Obama continúa, "la pregunta nunca ha sido si Estados Unidos debe tener o no el liderazgo internacional, la pregunta es cómo".[159] En lo que refiere a la seguridad cibernética "nosotros [Estados Unidos] estamos moldeando los estándares globales para la seguridad cibernética, estamos en construcción de la capacidad internacional para quebrantar e investigar las amenazas cibernéticas."[160]

2.1.4 El discurso en el Newseum

Para continuar con el discurso oficial ya no en el marco de las estrategias de Seguridad Nacional, pero sí en lo que refiere al espacio cibernético, en enero de 2010 la entonces Secretaria de Estado, Hillary Rodham Clinton, dio en el Newseum[161], Washington, un discurso

---

[157] Barack H. Obama, *The National Security Strategy of the United States of America February 2015*, Seal of the President of the United States, http://nssarchive.us/wp-content/uploads/2015/02/2015.pdf, 35 pp.

[158] Barack H. Obama, *The National Security Strategy of the United States of America February 2015,* p. 3.[traducción propia]

[159] Ídem.

[160] *Ibíd.,* p.4. [traducción propia]

[161] El Newseum es un museo e instituto con sede en Washington D.C. Se dedica a estudiar y defender el derecho a la libertad de prensa de acuerdo a la Primera Enmienda. Para mayor información, la página en línea del Newseum y del

acerca de la libertad de Internet que se volvió icónico por las incongruencias en comparación a lo que serían después las declaraciones con relación al caso Snowden. El discurso se encuentra íntegro en la página de Internet del Departamento de Estado en la sección de Diplomacia en Acción.[162] Se resaltan las siguientes ideas:

> En muchos aspectos, la información nunca ha sido tan libre como ahora. Hay más maneras de propagar las ideas a más gente que en cualquier otro momento de la historia. Incluso en países autoritarios, las redes de información ayudan a las personas a descubrir nuevos hechos que hacen que los gobiernos actúen de forma más responsable.
>
> […] Estas herramientas también son explotadas para socavar el progreso humano y los derechos políticos. […] las redes modernas de información y las tecnologías pueden ser aprovechadas para bien o para mal. Las mismas redes que ayudan a organizar movimientos para la libertad, también le permiten a *Al-Qaeda* pronunciarse con odio e incitar a la violencia en contra de los inocentes. Las mismas tecnologías con el potencial de abrir el acceso a los gobiernos y promover la transparencia, en sentido contrario, pueden ser secuestradas por gobiernos para aplastar la disidencia y negar los derechos humanos.
>
> Por sí mismas, las nuevas tecnologías no toman partido en la lucha por la libertad y el progreso, pero Estados Unidos sí. Defendemos un Internet en el que toda la humanidad tenga igualdad de acceso al conocimiento y las ideas. […]
>
> […] Algunos países han levantado barreras electrónicas para prohibir a su gente entrar a partes de las redes mundiales. […] Han violado la privacidad de ciudadanos que participan en un discurso político no violento. Estas acciones van en contra de la Declaración de Derechos Humanos, que nos dice que todas las personas tenemos derecho a buscar, recibir y compartir información e ideas por cualquier medio sin importar las fronteras. […] Como en las dictaduras del pasado, algunos gobiernos van contra pensadores independientes que usan estas herramientas […] Las alteraciones en estos sistemas demandan respuestas coordinadas de todos los gobiernos, el sector

Newseum Institute es la siguiente: www.newseuminstitute.org/

[162] En inglés: *Diplomacy in Action*

privado y la comunidad internacional.[163]

2.2 Guerra cibernética

Para comprender la guerra cibernética primero tenemos que tener claridad en qué es Internet, qué es el espacio cibernético y cómo funcionan. Richard A. Clarke, quien fue asesor en seguridad cibernética para la campaña presidencial de Barack Obama, explica que "el espacio cibernético lo conforman todas las redes informáticas del mundo y todo lo que ellas conectan y controlan. No se trata sólo de Internet. Es importante dejar en claro la diferencia. Internet es una red de redes abierta. Desde cualquier red de Internet, podemos comunicarnos con cualquier ordenador conectado con cualquier otra de las redes de Internet. El ciberespacio es Internet *más* montones de otras redes de ordenadores a las que, se supone, no es posible acceder desde Internet".[164] Aunque en el apartado anterior se mencionó la definición de espacio cibernético para el Departamento de Defensa, la definición de Clarke, al ser más sencilla, brinda mayor claridad.

2.2.1 Internet

En el caso particular de Internet, vale la pena tener claro que fue un invento estadunidense. Su precursor fue ARPANET, "[…] ante la posibilidad de un embate nuclear a finales de los sesenta, la Agencia de Investigación Avanzada del Departamento de Estados Unidos (DARPA), comisionó en 1967 a la Agencia de Proyectos de Investigación Avanzada (ARPA), la creación de una red para proteger los sistemas estratégicos y de información localizados en los núcleos y ciudades principales."[165]

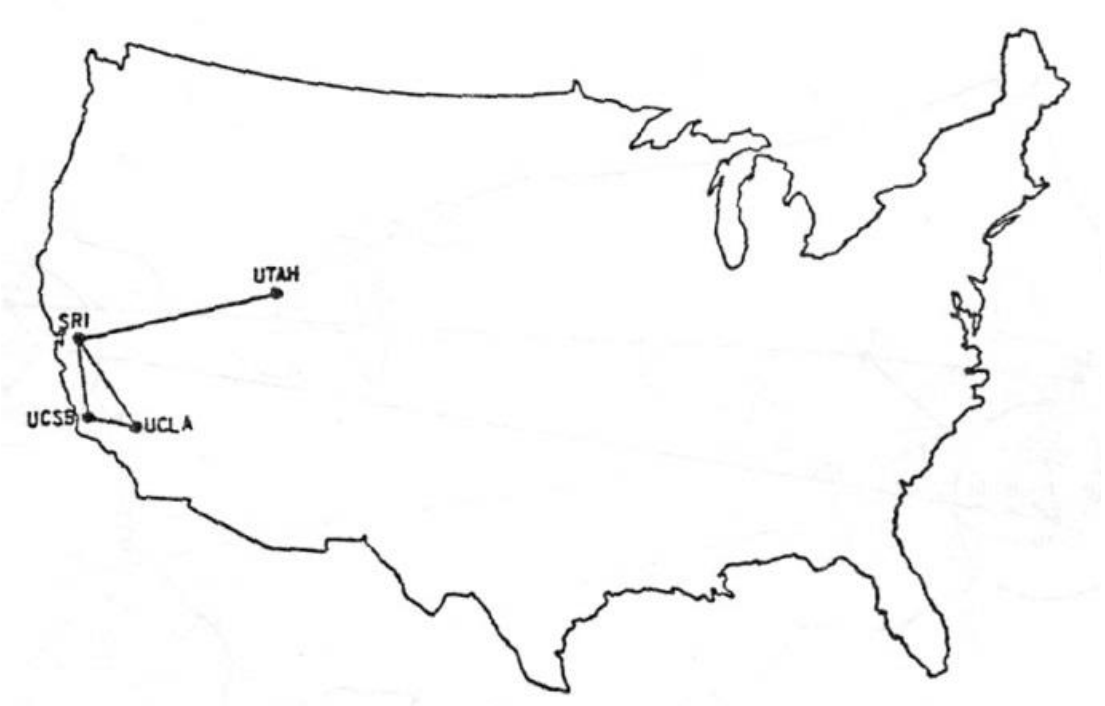
En 1969, como se muestra en el primero de los mapas que a continuación se exponen, surgió la primera red de redes entre universidades, llamada ARPANET. Las universidades que la componían fueron la Universidad de California en los Ángeles, UCLA; la Universidad de California en Santa Bárbara, UCSB; la Universidad de Stanford y la Universidad de Utah.

---

[163] Hillary Rodham Clinton, "Remarks on Internet Freedom", Electronic Frontier Foundation, martes 15 de febrero de 2011, https://www.eff.org/files/filenode/clinton_Internet_rights_wrongs_20110215.pdf [traducción propia]
[164] Richard A. Clarke, Robert K. Knake, Luis Alfonso Noriega (trad.), *Guerra en la red. Los nuevos campos de batalla*, Barcelona, Ariel, 2011, pp. 103 y 104.
[165] Adrián Estrada Corona, "Protocolos TCP/IP de Internet", Revista Digital Universitaria, Vol. 5, No. 8, 10 de septiembre de 2004, DGSCA-UNAM, p. 2.

ARPANET tenía "el propósito de apoyar las investigaciones militares, pues el gobierno de Estados Unidos necesitaba redes de comunicación que pudieran soportar daños como los causados por misiles."[166] Sin embargo también surgieron otras redes, CSNET y MILNET. "[…] la primera surgió con la finalidad de enlazar las computadoras de las áreas de investigación científica de las universidades, la industria y el gobierno, la segunda era una red militar del departamento de defensa de Estados Unidos. Con la unión de estas tres redes, en 1983 se inició el proyecto *Internetwork*. El término *Internetwork* se abrevió después para dar lugar a lo que hoy se conoce como Internet."[167]

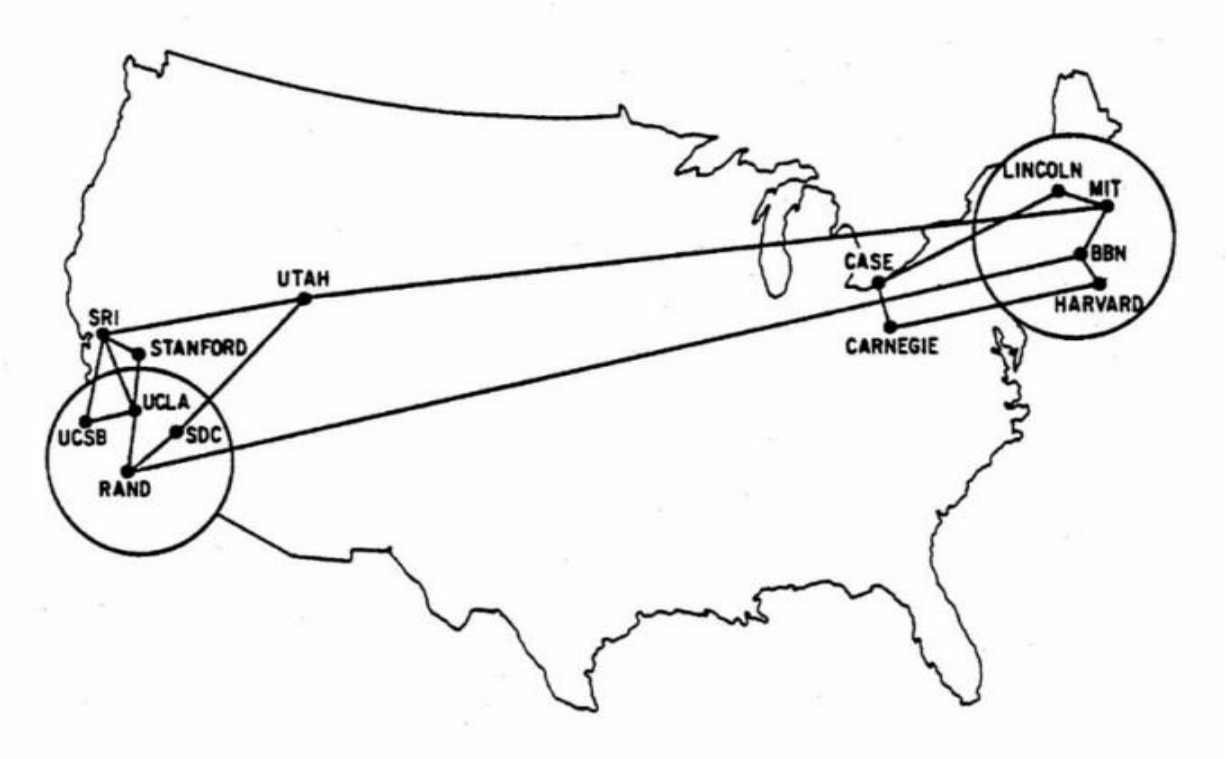
Internet fue pensado como modelo de comunicación para fines de investigación, suele decirse que académica, sin embargo, resulta difícil pensar que la agencia de la defensa encargada de la investigación tecnológica lo planeara así. Resulta más probable suponer que la conexión interuniversitaria fue un primer momento de prueba, los fines últimos siguen siendo desconocidos. La evolución de Internet:



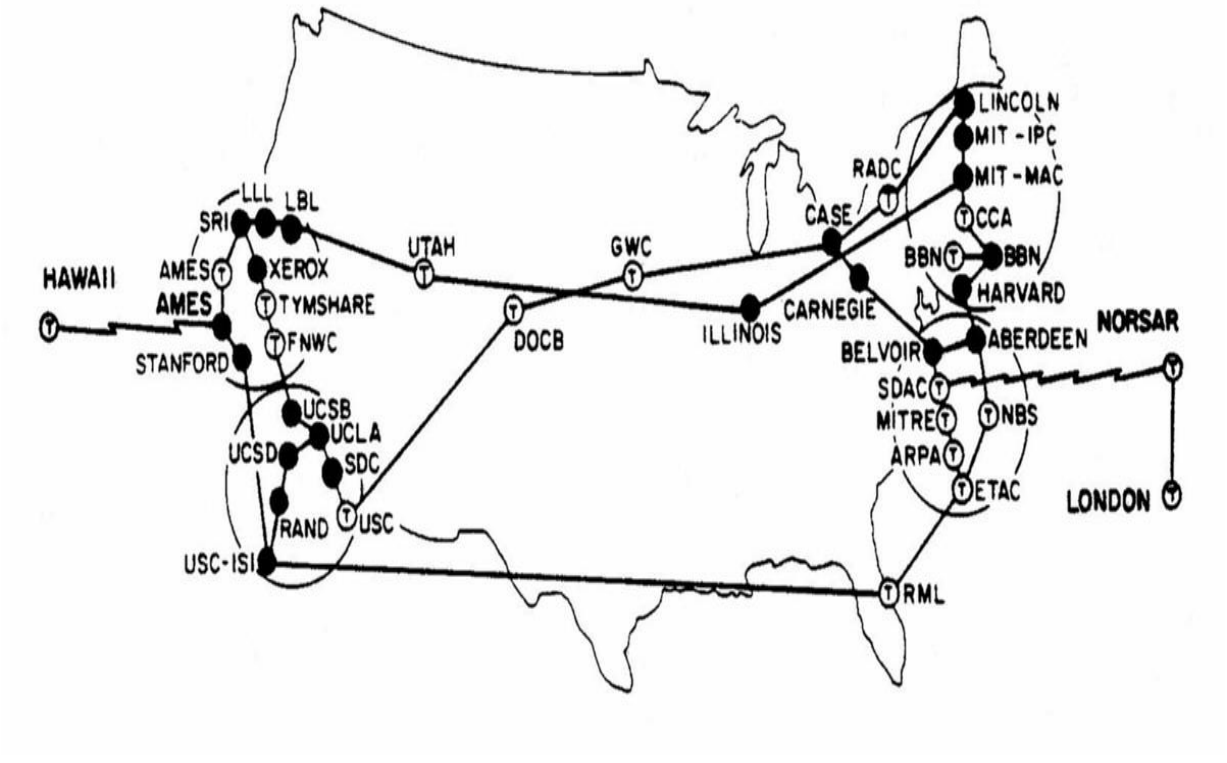
The ARPANET in December 1969

1969

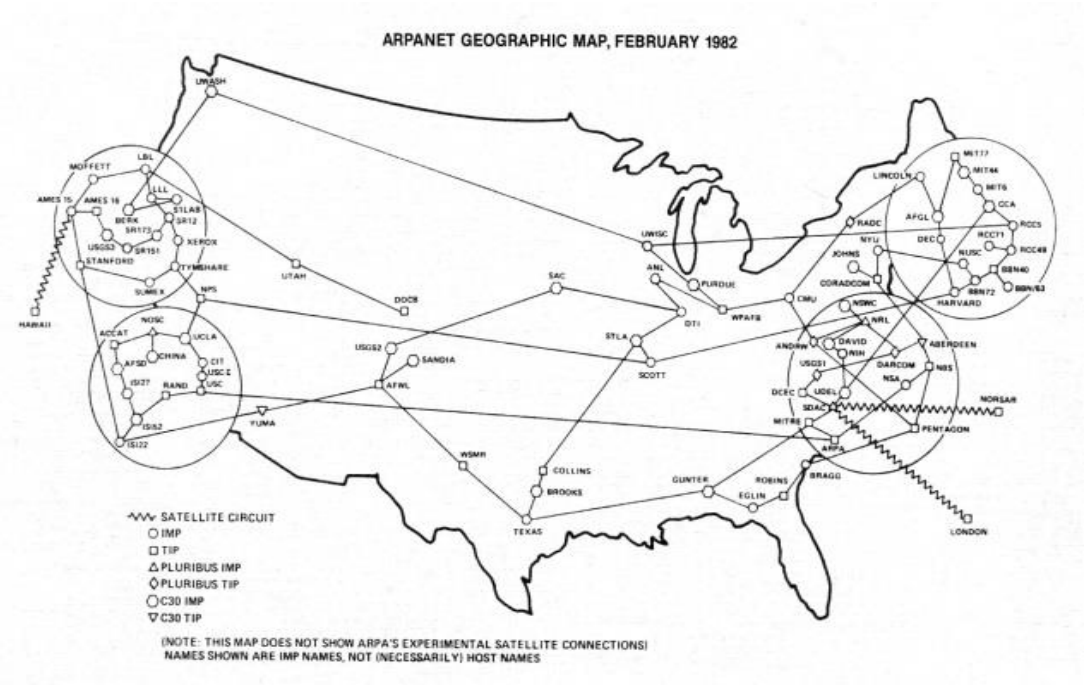
[166] *Ídem.*
[167] *Ídem.*


LINCOLN
MIT
BBN
HARVARD
CASE
CARNEGIE
UTAH
SRI
STANFORD
UCLA
UCSB
SDC
RAND

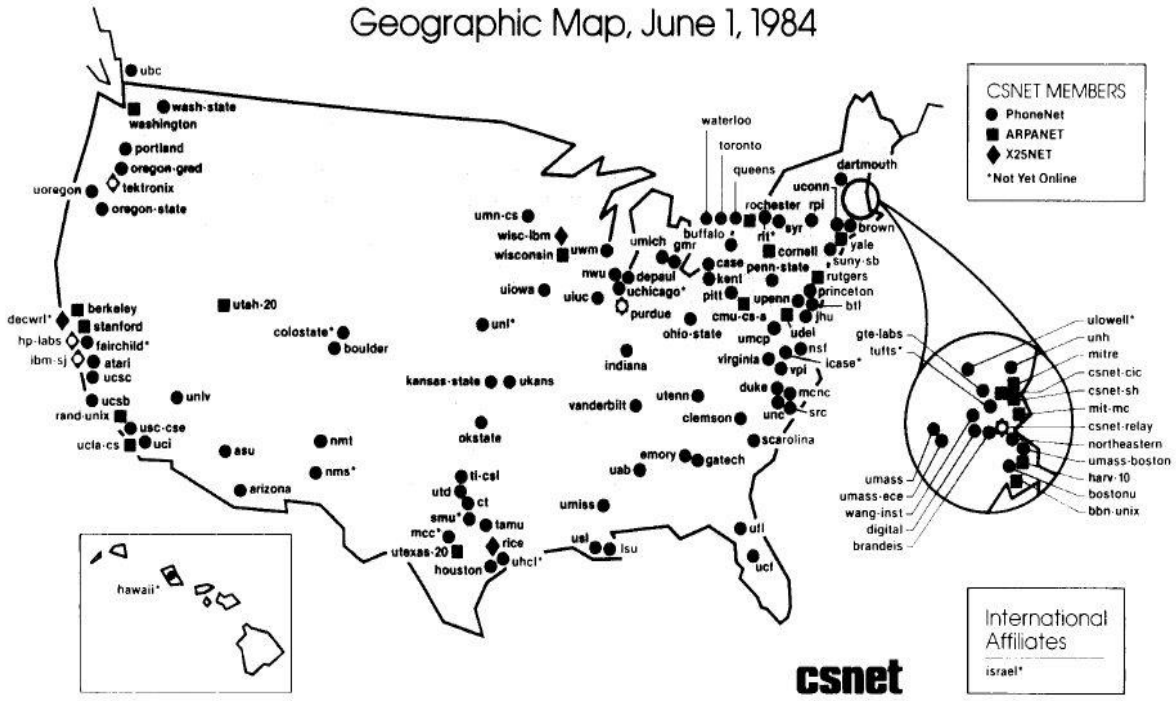
1970


LLL
LBL
SRI
AMES
XEROX
TYMSHARE
FNWC
HAWAII
AMES
STANFORD
UCSB
UCLA
UCSD
SDC
RAND
USC
USC-ISI
UTAH
GWC
DOCB
ILLINOIS
CASE
CARNEGIE
RADC
LINCOLN
MIT-IPC
MIT-MAC
CCA
BBN
BBN
HARVARD
ABERDEEN
NORSAR
BELVOIR
SDAC
MITRE
NBS
ARPA
ETAC
LONDON
RML

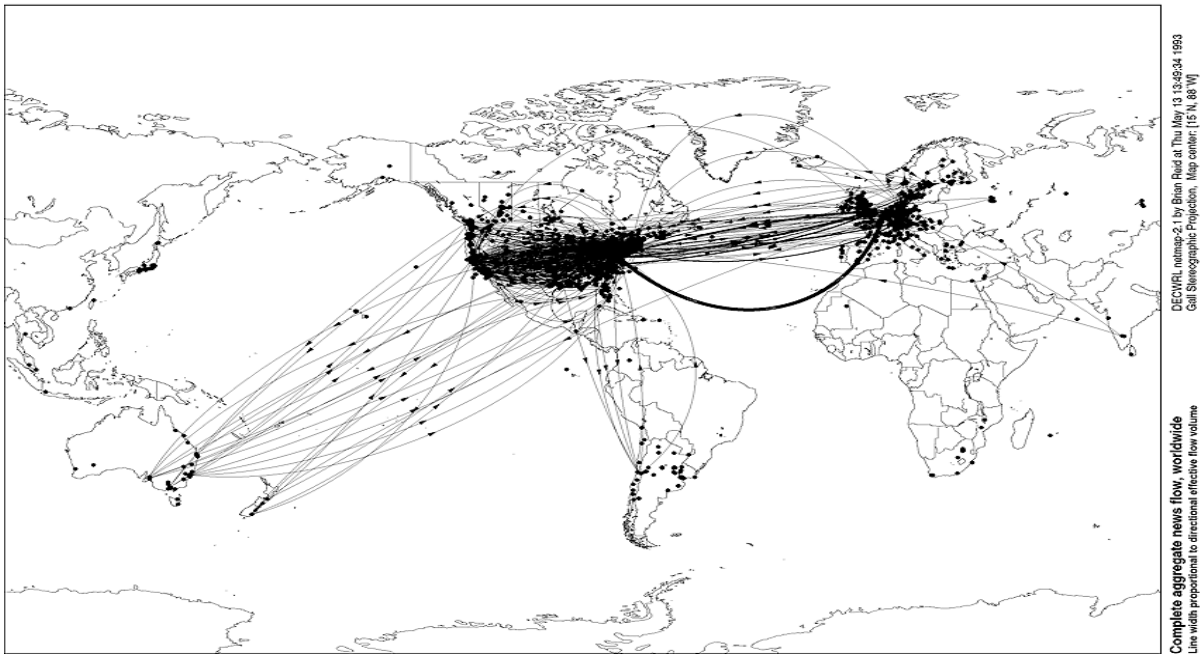
1973


ARPANET GEOGRAPHIC MAP, FEBRUARY 1982
SATELLITE CIRCUIT
IMP
TIP
PLURIBUS IMP
PLURIBUS TIP
C30 IMP
C30 TIP
(NOTE: THIS MAP DOES NOT SHOW ARPA'S EXPERIMENTAL SATELLITE CONNECTIONS)
NAMES SHOWN ARE IMP NAMES, NOT (NECESSARILY) HOST NAMES

1982


Geographic Map, June 1, 1984
CSNET MEMBERS
PhoneNet
ARPANET
X25NET
*Not Yet Online
International Affiliates
israel*
csnet

1984



Fuente: Timothy B. Lee, "40 maps that explain the Internet", Vox [168]

2.2.2 Espacio cibernético

Existe otra parte del ciberespacio la cual "permite que las máquinas hablen con otras máquinas como lo son los tableros de control con las bombas, los elevadores y los generadores",[169] esta parte es fundamental para las armas cibernéticas.

Los conceptos que aparecen en el diccionario del DoD, sobre esta materia son: seguridad cibernética, operaciones en el espacio cibernético y superioridad en el ciberespacio. Para poder definir guerra cibernética, comencemos por analizar lo que el Departamento de Defensa entiende por estos tres conceptos:

1. Seguridad cibernética. Prevención del daño, protección y restauración de computadoras; sistemas de comunicaciones electrónicas; servicios de comunicaciones electrónicas, incluyendo la información allí dentro para asegurar su disponibilidad, integridad, autenticidad, confidencialidad y certificación.[170]
2. Operaciones en el espacio cibernético. También llamadas CO, son el uso de las capacidades ciberespaciales donde el principal objetivo es lograr lo propuesto en o a

[168] Timothy B. Lee, "40 maps that explain the Internet", Vox, junio de 2014, https://www.vox.com/a/Internet-maps [traducción propia]
[169] Richard A. Clarke, Robert K. Knake, Luis Alfonso Noriega (trad.), *Guerra en la red. Los nuevos campos de batalla*. p. 104.
[170] *Dod Dictionary of Military and Associated Terms, as of August 2017,* entrada: cybersecurity, p. 58. [traducción propia]

través del espacio cibernético; [171][y,]

3. Superioridad cibernética. El grado de dominio obtenido en el espacio cibernético por un grupo operativo que garantice la seguridad, conductos confiables de operaciones para ese grupo, así como para los grupos operativos terrestres, aéreos, marítimos y espaciales, en un tiempo y lugar específico sin la interferencia prohibitiva de un adversario.[172]

Como segundo punto de partida para entender la guerra cibernética, se toman dos definiciones de guerra. Según el *Dictionary of International Relations*[173], cuyos autores son profesores de la Universidad de Wales, Swansea; guerra se define como "violencia somática, directa entre dos actores estatales"[174]. En otra entrada del mismo concepto retoman la definición del realismo, "[…] la idea de que la violencia y la guerra son componentes intrínsecos del sistema internacional es la característica distintiva del realismo. Las formas de violencia pueden cambiar bajo la influencia de la tecnología."[175]

Desde la Filosofía, la guerra para "[…] Hobbes […] es el estado 'natural' de la humanidad, en el sentido de ser el estado al que quedaría reducida sin las reglas del derecho, o del cual intenta salir mediante estas reglas"[176]; en el sentido inverso, "[…] Hegel […] consideró a la guerra como una especie de 'juicio de Dios', del que se vale la providencia histórica para hacer triunfar la mejor encarnación del Espíritu en el mundo. Hegel afirmó por un lado que 'como el movimiento de los vientos preserva al mar de la putrefacción a la que lo reduciría una perdurable quietud, de igual manera reduciría a los pueblos una paz durable o también perpetua. […] Por otro lado, consideró que en el plano providencial de la historia del mundo, un pueblo sucede a otro en el encarnar, realizar o manifestar el Espíritu del mundo, dominando,

[171] *Dod Dictionary of Military and Associated Terms, as of August 2017,* entrada: cyberspace operations, p. 58. [traducción propia]
[172] *Dod Dictionary of Military and Associated Terms, as of August 2017,* entrada: cyberspace superiority, p. 58. [traducción propia]
[173] Graham Evans, Newnham Jeffrey, *Dictionary of International Relations*, Londres, Penguin Books, 1998, 623 pp.
[174] *Ibíd.,* p. 565.
[175] *Ídem.*
[176] Nicola Abbagnano, Pedro Torres Aguilar (rev.), José Esteban Calderón et al. (trad.), *Diccionario de filosofía. Actualizado y aumentado por Giovanni Fornero/Nicola Abbagnano,* México, D.F., Fondo de Cultura Económica, 2004, p. 536.

en nombre y por medio de esta superioridad a todos los otros pueblos"[177].

Ahora, para cerrar este apartado y pasar a analizar lo que podríamos considerar el arsenal de guerra cibernética de Estados Unidos, el Departamento de Defensa define un sistema de armas como "la combinación de una o más armas que tienen equipo, materiales, servicios o personal relacionado, así como los medios de utilización y ejecución requeridos para su autosuficiencia".[178] Un sistema de armas cibernéticas se encuentra dentro del arsenal militar estadunidense, ¿se puede tener arsenal de armas sin la intención latente de ir a la guerra?, recordemos que las formas de violencia en la guerra cambian conforme cambia la tecnología.

2.2.3 El arsenal para la ciberguerra

Por todo lo anterior, hay certeza en que el espacio cibernético es un lugar en disputa. Sería el quinto dominio de guerra, después de tierra, mar, aire y el espacio. La incógnita reside en saber cuáles son las armas que posee Estados Unidos para imponer su hegemonía en este nuevo lugar. Cabe aclarar, la información oficial en lo que respecta a las armas puntuales utilizadas, es escasa.

Sin embargo, se cuenta con investigaciones e información que surgió gracias al periodismo de investigación o a filtraciones publicadas por WikiLeaks. Así fue como se pudo investigar cuáles armas cibernéticas apuntan a Estados Unidos.

El 8 de julio de 2015, WikiLeaks publicó "[…] más de un millón de correos electrónicos del vendedor italiano de *malware* para la vigilancia, *Hacking Team.* Esta empresa saltó a la vista del escrutinio internacional después de la publicación por WikiLeaks de los *SpyFiles*. Los correos electrónicos de *Hacking Team* muestran el trabajo interno de la controversial industrial de la vigilancia global".[179] Ahí se encuentran múltiples referencias sobre las armas cibernéticas y su uso.

Stuxnet, Duqu y *Flame*, ponen sobre la mesa la capacidad destructiva de las armas cibernéticas. Dos de los problemas que surgen para entender esta clase de armas son, uno, la tecnología avanza a una velocidad mayor que el análisis académico y, dos, la información del

[177] *Ídem.*
[178] *Dod Dictionary of Military and Associated Terms, as of August 2017*, entrada: weapon system, p. 248. [traducción propia]
[179] s/a, "*Hacking Team*", WikiLeaks, 8 de julio de 2015, https://WikiLeaks.org/hackingteam/emails/. [traducción propia]

armamento actual aún no está a la luz pública. Por la información que sí se conoce es por dónde podemos mapear de qué va el uso de la tecnología armamentista en el ciberespacio y para qué se utiliza.

2.2.3.1 Stuxnet/Olympic Games

Stuxnet es un gusano cibernético o *malware*[180] que afecta el actuar de las computadoras. En específico, funciona para alterar los comandos o instrucciones dictados por computadoras a máquinas industriales; los modifica al introducir líneas de código dictadas por los creadores del virus. Stuxnet fue parte de una estrategia ofensiva más grande conocida como *Olympic Games*.

El uso de Stuxnet quedó documentado con la alteración a las actividades de centrifugadoras para el enriquecimiento de uranio, con las que se busca, una versión más pura del Uranio 235. Esto sucedió en la planta nuclear de Natanz, en Irán. "La existencia de la instalación [Natanz], fue expuesta en 2003".[181]

Lo que se sabe es decir, de lo que se tiene constancia, es que en enero de 2009, "oficiales de la Agencia Internacional de Energía Atómica [IAEA, por sus siglas en inglés], cuerpo de Naciones Unidas encargado de monitorear el programa nuclear de Irán, comenzó a notar que algo inusual sucedía en la planta de enriquecimiento de uranio de Natanz, en la parte central de Irán".[182]

Según los datos que se pudieron obtener, entre 800 y 1000, aunque hay cifras que llegan a 2000, centrifugadoras de Natanz, cuyo modelo es IR-1[183], fueron remplazadas por fallas indetectables hasta ese momento. Fue necesario que "más de una docena de expertos en seguridad cibernética de todo el mundo, pasaran meses en la deconstrucción de lo que se convertiría en el descubrimiento de uno de los virus más sofisticados, -una pieza de software tan particular que haría historia como la primer arma digital del mundo y la primera en anunciar la era de la guerra digital".[184]

¿Quién creo esta arma con la capacidad para sacar de funcionamiento cientos de

[180] Ver las entradas, gusano o virus informático y *malware*, en el glosario.
[181] David E. Sanger, "Chapter 8, Olympic Games", *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power*, *op.cit.,* p. 3 de 41. [traducción propia]
[182] Kim Zetter, *Countdown to Zero Day. Stuxnet and the launch of the world's first digital weapon*, Nueva York, Penguin Random House Company, 2014, p. 6. [traducción propia]
[183] *Ídem.*
[184] *Ibíd.,* p. 7. [traducción propia]

centrifugadoras de enriquecimiento de uranio? De acuerdo al artículo "Prueba israelí sobre gusano es crucial en retraso nuclear en Irán" (*Israeli Test on worm Called Crucial in Iran Nuclear Delay)*[185]*,* publicado por *The New York Times* en enero de 2011; el complejo Dimona situado en el desierto de Néguev, al sur de Israel, sirvió "como sitio de pruebas en un esfuerzo conjunto entre Estados Unidos e Israel para socavar los esfuerzos de Irán en la creación de una bomba [nuclear]".[186]

La operación en conjunto recibió el nombre de *Olympic Games*. "Los detalles de *Olympic Games,* sólo fueron conocidos por un grupo compacto de Inteligencia del más alto nivel, militares y oficiales de la Casa Blanca. La operación tenía dos objetivos. El primero, paralizar, al menos por un tiempo, el progreso nuclear en Irán. El segundo, de igual importancia, convencer a los israelíes, de la existencia de una manera más inteligente y más elegante de lidiar con el problema nuclear de Irán que lanzar un ataque aéreo que rápidamente podría escalar en otra guerra en Medio Oriente, que dispararía los precios del petróleo e involucraría a los jugadores más volátiles de la región".[187]

Las agencias encargadas de la Inteligencia de las comunicaciones de Israel y Estados Unidos, estuvieron presentes en la creación y desarrollo de Stuxnet, nombrado así por los trabajadores de las empresas de seguridad informática que más adelante investigarían al virus. "−Fue muy extraño, tenías a dos agencias que generalmente no juegan en equipo−, dijo un antiguo oficial de Inteligencia de Estados Unidos que trabajó con intensidad sobre Irán. Actuales oficiales, discuten si Irán fue el factor que acercó a la Inteligencia estadunidense e israelí más que nunca. Y, mientras 'el bicho', como lo llaman algunos estadunidenses, fue primero diseñado por una pequeña célula de guerreros cibernéticos de la NSA, pronto habría mejorías, otras versiones, que vendrían de la famosos Unidad 8200, el equivalente israelí de la NSA".[188]

En declaraciones, la entonces secretaria de estado Hillary R. Clinton y Meir Dagan[189],

---

[185] William J. Broad, John Markoff y David E. Sanger, "Israeli Test on Worm Called Crucial in Iran Nuclear Delay", Middle East, The New York Times, 15 de enero de 2011, https://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html [traducción propia]
[186] *Ídem.*
[187] David E. Sanger, "Chapter 8. Olympic Games", *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power*, *op. cit.,* p. 3 de 42. [traducción propia]
[188] *Ibíd.,* p. 9 de 42. [Traducción propia]
[189] Meir Dagan fue el director del Mossad de 2002 a 2011, esta información se encuentra en la *Jewish Virtual Library*,

director en ese entonces del Mossad, la agencia de Inteligencia israelí, afirmaron "que creían que los esfuerzos de Irán [en la construcción de la bomba atómica] habían sido retrasados años".[190] Meir Dagan declaró ante el Knesset, la asamblea de Israel, "Irán se ha encontrado con dificultades tecnológicas, mismas que podrían retrasar la bomba hasta 2015."[191] Es pertinente traer a colación que el Mossad, "ha sido acusado por Irán de estar detrás de la muerte de varios científicos iraníes". [192]

Las centrifugadoras en el complejo de Natanz, tenían como controlador un software de la empresa alemana Siemens. "A principios de 2008, […] Siemens cooperó con el laboratorio nacional de Idaho [este laboratorio forma parte del Departamento de Energía de Estados Unidos] para identificar las vulnerabilidades de los controladores. Mismos, que la compañía vende alrededor del mundo para operar maquinaria industrial, −las agencias de Inteligencia de Estados Unidos, lo han identificado como equipo clave de las instalaciones de enriquecimiento de uranio en Irán".[193] Siemens argumentó que cooperó con el gobierno estadunidense para investigar las fallas del software y así poder aumentar su ciberseguridad. Sin embargo, "estos bien escondidos agujeros [fallas del software], fueron explotados al año siguiente, por Stuxnet".[194]

En el mundo de la política, cuando no se tiene certeza de un hecho, las declaraciones forman una pista más del complicado enjambre de puntos que se unen para saber de dónde proviene una acción, por ejemplo, cuando sucedió el ataque a Natanz, el entonces presidente de Estados Unidos, Barack Obama no hizo ninguna declaración, sin embargo, "[…] el jefe de asesores en armas de destrucción masiva y control de armas, Gary Samore, […] dijo 'estoy contento de escuchar que tengan [el gobierno de Irán] problemas con sus centrifugadoras, Estados Unidos y sus aliados hacen todo lo que puede para que las cosas se le compliquen aún más".[195]

En 2008, cuando comenzaron a fallar las centrifugadoras, compañías de seguridad

---

ww.jewishvirtuallibrary.org/directors-of-the-national-intelligence-agency-mossad

[190] William J. Broad, John Markoff y David E. Sanger, "Israeli Test on Worm Called Crucial in Iran Nuclear Delay", *op. cit.*

[191] *Ídem.*

[192] Ídem.

[193] *Ídem.*

[194] *Ídem.*

[195] Kim Zetter, *Count down to zero day. Stuxnet and the launch of the world's first digital weapon*, *op. cit.,* p. 159. [traducción propia]

informática se dedicaron a investigar el nuevo virus que andaba suelto en el internet del mundo. Especialistas en seguridad cibernética tardaron meses en poder deconstruir Stuxnet y así saber de qué trataba este bicho malicioso y a quien había infectado. Las empresas clave para la deconstrucción del mismo, fueron la alemana Symantec y la rusa Kaspersky.

2.2.3.2 *Flame*

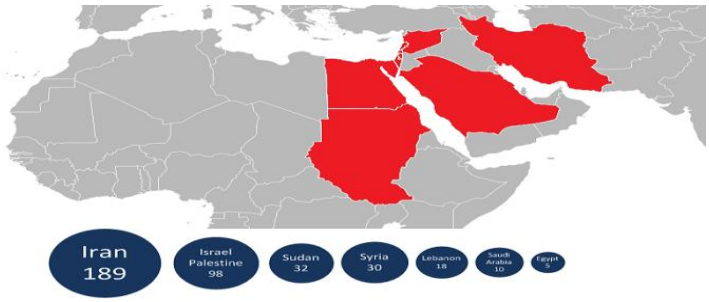
Flame es un arma cibernética que fue descubierta por Kaspersky Lab. Alexander Gostev quien funge como director y es experto en seguridad del equipo en búsqueda global y análisis de esta empresa, cuyo trabajo se enfoca en la seguridad cibernética global, escribió el artículo nombrado "*Flame*: preguntas y respuestas"[196]. En este artículo A. Gostev especifica que Kaspersky Lab encontró el *malware* de espionaje cibernético conocido como *Flame* cuando la "Unión Internacional de Telecomunicaciones de la ONU les pidió ayuda en encontrar otro *malware* que estaba borrando información sensible en Medio Oriente. Mientras [buscaban] ese código […] encontraron un nuevo *malware* cuyo nombre en código era Worm.Win32.*Flame*."[197]

Lo que pudo saber Kaspersky Lab respecto a los autores de *Flame* y de si el *malware* había sido creado por un gobierno, hacktivistas o criminales cibernéticos, Alexander Gostev lo respondió de la siguiente manera, "actualmente hay tres clases de actores que desarrollan *malware* y *spyware*: los hacktivistas, los criminales cibernéticos y los Estados-nación. *Flame* no está diseñado para robar dinero de cuentas bancarias. También es diferente de herramientas simples de hackeo y *malware* que utilizan los hacktivistas. Así que, si excluimos a los criminales cibernéticos y a los hacktivistas, llegamos a la conclusión que seguramente pertenece al tercer grupo. Además, la geografía de los objetivos (ciertos Estados de Medio Oriente), y también la complejidad de la amenaza, no deja duda de que fue un Estado-nación el que patrocinó la investigación [para la creación de *Flame*]".[198]

Los países que sufrieron ataques de *Flame* fueron Irán, Palestina, Libia, Siria, Sudán, Arabia Saudita y Egipto. A continuación se muestra el mapa de los países con la cantidad de

[196] En inglés:"The *Flame*: Questions and Answers"
[197] Alexander Gostev, "The *Flame*: Questions and Answers", Incidents, Secure List, 20 de mayo de 2012, https://securelist.com/the-*Flame*-questions-and-answers-51/34344/ [traducción propia]
[198] *Ídem.*

ataques recibidos hasta mayo de 2012, fecha de la publicación del artículo de Alexander Gostev.



Fuente: Karspersky Lab

El lema de la empresa de vigilancia, *Hacking Team*, es "El juego del hackeo para la interceptación gubernamental" (*The Hacking suite for governmental interception*); según se lee en su página oficial, actúan con los siguientes principios "Nosotros creemos que luchar contra el crimen debería ser sencillo: proveemos tecnología efectiva y fácil de usar a los cuerpos de seguridad y a las comunidades de Inteligencia del mundo entero",[199] aclaran que sólo venden su tecnología a gobiernos.

En el correo electrónico filtrado y publicado por WikiLeaks "*Researchers Connect Flame to US-Israel Stuxnet Attack*"[200] enviado por vince@hackingteam.it para list@hackingteam.it con fecha del 6 de diciembre de 2012 se hace referencia a un artículo publicado por la revista *Wired* cuyo título es igual al del correo electrónico. Los miembros de *Hacking Team* que enviaron el correo electrónico subrayan un párrafo que dice así: "El sofisticado juego de herramientas de espionaje conocido como *Flame* está directamente relacionado con Stuxnet, el súper gusano que atacó las centrifugadoras de Irán en 2009 y 2010. De acuerdo a los investigadores quienes […] encontraron que el módulo principal en *Flame* contiene código que es casi idéntico a un módulo que se usó en una temprana versión de Stuxnet". [201]

A pesar de que ese párrafo es el que resaltan los integrantes de *Hacking Team*, el artículo que fue escrito por Kim Zetter en noviembre de 2012, contiene una radiografía de las funciones

[199] s/a, "Customer policy" , *Hacking Team*, http://www.hackingteam.it/policy.html
[200] "Researchers Connect *Flame* to US-Israel Stuxnet Attack", Email-ID 598638, 2012-06-12, de: vince@hackingteam.it, para: list@hackingteam.it, https://WikiLeaks.org/hackingteam/emails/emailid/598638 [traducción propia]
[201] *Ídem.*

del arma.

> - El *malware* […] ha estado activo por lo menos dos años. Los investigadores descubrieron que puede ser utilizado para robar documentos, leer comunicaciones escritas que ocurran en una computadora o grabar conversaciones que ocurran en Skype o en los alrededores de una computadora infectada [vía bluetooth].
> - Hasta ahora, los investigadores [de Karspersky Lab] creían que *Flame* probablemente era parte de un proyecto paralelo creado por contratistas que trabajaban para el mismo equipo del Estado-nación detrás de Stuxnet y su *malware* hermano DuQu […] Ahora creen que los creadores de Stuxnet usaron parte de *Flame* en una etapa temprana de Stuxnet […]
> - El equipo que trabajó en Stuxnet construyó este *malware* para que fuera un arma cibernética de sabotaje, mientras que el equipo que trabajó en *Flame* tomó el módulo que apareció en Stuxnet y construyó lo que se convertiría en la herramienta de espionaje masivo que Kaspersky descrubrió […].[202]

Flame también llamó la atención de académicos. Por ejemplo, Chris Bronk, quien es miembro de la Universidad de Rice en Houston Texas en el Instituto Baker de Políticas Públicas en el área de políticas de tecnología de la información; en un artículo que aparece en la página de la escuela Munk de Asuntos Internacionales de la Universidad de Toronto que se intitula "Intriga cibernética: la política internacional del *malware Flame*" (*Cyber Intrigue: The Flame Malware International Politics*), Chris Bronk señala que *Flame* se encontró "[…] en computadoras de Medio Oriente desde Irán hasta los territorios ocupados de Palestina. Posiblemente sea el *malware* que se detectó en la refinería de petróleo y complejo de exportación iraní en la isla de Kharg"[203].

Chris Bronk argumenta lo mismo que con anterioridad señaló Kaspersky Lab, "de acuerdo con algunos reportes, los iraníes llevaron *Flame* a la Unión Internacional de

[202] Kim Zetter, "Researchers connect *Flame* to US-Israel Stuxnet attack", Wired, 6 noviembre de 2012, https://www.wired.com/2012/06/*Flame*-tied-to-stuxnet [traducción propia]
[203] Chris Bronk, "Cyber Intrigue: The *Flame Malware* International Politics", Munk School of Global Affairs, The University of Toronto, 31 de mayo de 2012, http://www.cyberdialogue.ca/2012/05/cyber-intrigue-the-*Flame-malware*-international-politics/ [traducción propia]

Telecomunicaciones (ITU, por sus siglas en inglés), un cuerpo de Naciones Unidas. […] Los oficiales de ITU llamaron a Kaspersky Lab […] para estudiar *Flame*. […] Todo esto se suma a una historia que tiene más que ver con la política internacional en torno a una pieza de *malware* que con el *malware* mismo. Gracias a Stuxnet, la agenda de libertad de internet y la primavera árabe, el espacio cibernético es ahora un espacio político e importa mucho en las relaciones internacionales".[204]

2.2.3.3 El sistema Quantum y Foxacid

A diferencia de Stuxnet y *Flame*; Quantum y Foxacid no alteran el comportamiento de los controladores de una computadora. Es decir, no se instalan en la parte física del equipo, en cambio, alteran el comportamiento del funcionamiento en internet, en particular de los buscadores. Pero no de todas las herramientas de búsqueda comunes como Google, Opera, Safari, etc., Quantum y Foxacid tienen como objetivo específico una herramienta de búsqueda con contenido ético, Tor.

Tor es un *software*[205] y una red cuya principal función es ser un motor de búsqueda seguro para sus usuarios. Su lema es, "protegemos la privacidad de millones cada día. Tor: empoderando la resistencia digital".[206] Esta herramienta es usada por defensores de derechos humanos, periodistas, filtradores e incluso gobiernos, para asegurar que sus búsquedas no pueden ser espiadas ni su localización detectada a través de su conexión a internet.

En octubre de 2013, Bruce Schneier, jefe de tecnología de IBM Resilient, miembro del Centro Berkman en Harvard y parte de la junta de la Fundación De la Frontera Electrónica, EFF, por sus siglas en inglés, publicó el artículo "La NSA ataca a los usuarios de Tor/Firefox con Quantum y Foxacid" (*How the NSA Attacks Tor/Firefox Users With Quantum and FOXACID*). Este artículo se consiguió en WikiLeaks en la sección de documentos: *Hacking Team*, misma que engloba archivos que giran alrededor de la industria de la vigilancia. El artículo originalmente fue publicado en el blog *www.schneier.com*, sin embargo la dirección ya no existe. Queda constancia del artículo en WikiLeaks con los siguientes datos:

[204] *Ídem.*
[205] Software, entrada en glosario.
[206] https://www.torproject.org/

How the NSA Attacks Tor/Firefox Users With QUANTUM and FOXACID

Email-ID	66482
Date	2013-10-08 02:40:31 UTC
From	d.vincenzetti@hackingteam.com
To	list@hackingteam.it

207

Schneier lo explica así, "El trabajo para atacar Tor lo realiza la rama de vulnerabilidades de la NSA, esta rama es parte del directorio de sistemas de Inteligencia o SID [por sus siglas en inglés]. La mayoría de los empleados de la NSA trabajan en el SID, encargado de la recolección de información de los sistemas de comunicación alrededor del mundo".[208]

Schenier llegó a estas conclusiones acerca del uso de Quantum y Foxacid a causa de filtraciones de información confidencial, "[…] De acuerdo a una de las presentaciones de la NSA clasificadas *top-secret* y filtradas por Edward Snowden, una de las técnicas exitosas que la NSA ha desarrollado [… es la de] identificar a los usuarios de Tor en Internet y luego ejecutar un ataque contra su buscador Firefox. La NSA se refiere a estas capacidades como explotación de redes computacionales o CNE [por sus siglas en inglés]".[209]

Resulta interesante notar el uso del término capacidades de explotación de redes computacionales; uno de los significados que podemos encontrar en el Diccionario de la lengua española del término capacidad es: "oportunidad, lugar o medio para lograr algo"[210], en este sentido, la oportunidad de explotar las redes computacionales para obtener información se da a través del uso de una herramienta fabricada, Quantum y Foxacid, para dinamitar un lugar seguro, Tor, para fines concretos.

Sin el afán de entrar en cuestiones técnicas de la manera en que opera el SID, en la consecutiva cita se da un marco amplio de cómo funcionan estas ¿armas?, de la NSA. "El primer paso de este proceso [que se refiere a implantar Quantum y Foxacid subrepticiamente], consiste en encontrar usuarios de Tor. Para lograrlo, la NSA se apoya en su vasta capacidad para monitorear grandes partes de internet. Esto se hace vía las colaboraciones de la agencia con firmas de telecomunicaciones estadunidenses cuyos nombre en código son *Stormbrew,*

---

[207] "How the NSA Attacks Tor/Firefox Users With Quantum and FOXACID", Email-ID 66482, 2013-10-08, de d.vincenzetti@hackingteam.com, para: list@hackingteam.it, *Hacking Team* Archive, WikiLeaks, https://WikiLeaks.org/hackingteam/emails/emailid/6648

[208] *Ídem.*

[209] *Ídem.*

[210] Diccionario de la Lengua Española, Real Academia Española, en línea, entrada: "capacidad".

Fairview, Oakstar y *Blarney".*[211]

Otro concepto que refiere a las nuevas tecnologías y su uso es el de guerrero cibernético. Richard A. Clarke quien forma parte de la élite política de Estados Unidos, escribió que "cuando un hacker[212] hace algo como entrar en un sitio en el que no está autorizado, se convierte en un criminal cibernético o cibercriminal. Cuando trabaja para las fuerzas armadas de Estados Unidos, los llamamos ciberguerreros."[213]

2.3 La divina red

La divina red cumple con dos funciones. La primera hace referencia al concepto de Sun Tzu en su libro *El arte de la guerra*; en él, argumenta que los agentes secretos que trabajan para obtener información previa a una invasión en tiempos de guerra, constituyen la riqueza más preciada de un soberano.[214] La segunda, es trasladar el concepto de Sun Tzu a la contemporaneidad; Estados Unidos mantiene una relación similar con las compañías de las tecnologías de las comunicaciones. Éstas, además de tener como objetivo ampliar su mercado e impulsar la capacidad tecnológica del país, utilizan sus ventajas técnicas para proporcionar información a la Comunidad de Inteligencia. De ahí que sean "la divina red" de Estados Unidos.

En los años sesenta del siglo XX el sociólogo estadunidense C. Wright Mills propuso en su libro *La élite del poder,* una interpretación para comprender el ejercicio del poder en Estados Unidos. Lo que Mills argumentó es que el poder en Estados Unidos se concentra en una élite formada por una yuxtaposición del poder económico, político y militar, esta interpretación concuerda con la postura analizada durante la presente investigación.

> […] Las decisiones de un puñado de empresas influyen en los acontecimientos militares, políticos y económicos en todo el mundo. Las decisiones de la institución

[211] "How the NSA Attacks Tor/Firefox Users With Quantum and FOXACID", Email-ID 66482, 2013-10-08, de d.vincenzetti@hackingteam.com, para: list@hackingteam.it, *Hacking Team* Archive, WikiLeaks, https://WikiLeaks.org/hackingteam/emails/emailid/66482

[212] Hacker, ver entrada en el glosario.

[213] Richard A. Clarke, Robert K. Knake, Luis Alfonso Noriega (trad.), *Guerra en la red. Los nuevos campos de batalla, op.cit.,* p. 107.

[214] *El arte de la guerra,* "fue redactado entre los años 400 y 320 antes de Jesucristo". Sun Tzu, *El arte de la guerra,* Ciudad de México, Casa editorial Boek México, s/ año, p. 6

> militar descansan sobre la vida política así como sobre el nivel mismo de la vida económica, y los afectan lastimosamente. Las decisiones que se toman en el dominio político determinan las actividades económicas y los programas militares.
> […] Si hay intervención gubernamental en la economía organizada en grandes empresas, también hay intervención de esas empresas en los procedimientos gubernamentales. En el sentido estructural, este triángulo de poder es la fuente del directorio entrelazado que tanta importancia tiene para la estructura histórica del presente.[215]

Otra interpretación de la monopolización del poder en Estados Unidos, es el argumento histórico del desarrollo de las fuerzas de producción para sustentar la relación entre ejercicio de gobierno y poder económico, en el caso de este estudio, la fuerza económica de las empresas de las comunicaciones. Por ejemplo,

> Los laboratorios de ATT en Estados Unidos (los Bell Labs) decidirán a fines de los años treinta [del siglo XX] trabajar en los componentes sólidos. Estas investigaciones interrumpidas durante la guerra, desembocarán en 1947 en la puesta a punto del primer transistor de punta de germanio. […] En 1955, los laboratorios Bell lanzan los transistores que constituirán la base de la informática, de las telecomunicaciones digitales y, de forma más general, de la electrónica.[216]

La cita anterior muestra la manera en que las empresas de las comunicaciones han ido evolucionando conforme las investigaciones científicas y técnicas les han permitido, esto a su vez se inmiscuyó en el Estado, en particular en sus aplicaciones técnicas en el ámbito militar. En este punto cabe preguntarnos qué tan inmiscuido están tanto el Estado como las empresas, en el desarrollo técnico-científico del avance de las comunicaciones; "La evolución técnica a largo plazo se manifiesta así mediante la búsqueda continua de unas prestaciones propias de un

[215] C. Wright Mills, Florentino M. Turner, Ernestina de Champourcin (trad.), *La élite del poder*, México, D.F., Fondo de Cultura Económica, 1973, p. 15.
[216] Flichy Patrice, Eugeni Rosell i Miralles (trad.) *Una historia de la comunicación moderna. Espacio público y vida privada*, San Adrián de Besós, G. Gili, 1993, p. 168.

sector tecnificado […], que se inscribe en la evolución secular del capitalismo industrial: incremento de la productividad del trabajo mediante la mecanización y la automatización."[217]

2.3.1 El discurso de Eisenhower

Dwight D. Eisenhower fue presidente de Estados Unidos durante dos periodos, de 1953 a 1961. En el marco de la Guerra Fría, antes de ocupar el cargo de presidente, fue el primer comandante supremo de la Organización del Tratado del Atlántico Norte, OTAN. Durante su mandato como presidente de Estados Unidos, "una resolución en conjunto del Congreso, proclamó en 1957 la Doctrina Eisenhower. Ésta autorizaba al presidente asistir a cualquier nación de Medio Oriente que se juzgara que era amenazada por agresiones comunistas."[218]A pesar de lo anterior, lo que interesa resaltar aquí es lo siguiente: el 17 de enero de 1961 en su discurso de despedida, se dirigió a Estados Unidos por última vez como presidente. Ahí, se acuñó el término industria militar, por esta razón el discurso se volvió célebre.

> Un elemento vital para mantener la paz es nuestro arraigo militar. Nuestras armas deben ser poderosas, estar listas para la acción instantánea para que ningún potencial agresor esté tentado a correr el riesgo de su propia destrucción.
>
> Hasta el último de los conflictos mundiales, Estados Unidos no tenía industria armamentista […] nos hemos visto obligados a crear una industria armamentista permanente de vastas proporciones […] Anualmente gastamos más en seguridad militar que el total del ingreso neto de todas las corporaciones estadunidenses.
>
> Esta conjunción de un inmenso establecimiento militar y una gran industria armamentista, es nueva en la experiencia estadunidense. […] Reconocemos la imperiosa necesidad de este desarrollo, pero no debemos fallar en comprender sus graves implicaciones. Nuestros trabajos, recursos y forma de vida están involucrados, así como la estructura de nuestra sociedad. Desde el gobierno debemos protegernos contra la adquisición de influencia innecesaria buscada o no buscada por el complejo militar-industrial.[219]

---

[217] *Ibíd,* p. 161.
[218] Graham Evans, Jeffrey Newnham, *Dictionary of International Relations*, entrada: "Eisenhower Doctrine", Londres, Penguin Books, 1998, p. 146. [traducción propia]
[219] Dwight D. Eisenhower, "Farewell Address", en Ted Widemer, *American speeches. Political oratory from Patrick Henry*

Sin embargo, a causa de la importancia que adquirió el concepto complejo militar-industrial[220], se dejaron otros puntos del discurso fuera. Los cuales, desde la postura del presente escrito, no son de menor importancia. Eisenhower tampoco les dio una menor jerarquía.

> Semejante a, y en gran medida responsable de los avasalladores cambios en nuestra postura industrial-militar, ha sido la revolución tecnológica de las décadas recientes.
> En esta revolución la investigación se ha vuelto central, también se ha vuelto más formal, compleja y costosa. Un crecimiento constante es conducido para, por y bajo la dirección del gobierno federal.
> […] Las universidades libres, fuente histórica de ideas libres y descubrimientos científicos ha experimentado una revolución en la manera de investigar. En parte por los grandes costos involucrados, un contrato gubernamental se vuelve virtualmente el sustituto de la curiosidad intelectual. Por cada viejo pizarrón hay ahora cientos de nuevas computadoras electrónicas.[221]

D. Eisenhower fue más allá, vio peligro en la conformación de este nuevo grupo de interacción que se crea a partir de la inversión del gobierno en la investigación científica, y puso el ejemplo en las computadoras. "Aún con el respeto que merecen y que le debemos a la investigación y los descubrimientos, debemos estar alerta al peligro de que la política pública se pueda convertir en cautiva de una élite científica-tecnológica o viceversa."[222]

2.3.2 *Silicon Valley*

Desde una perspectiva geográfica *Silicon Valley* se localiza al norte de California, en la región sur de San Francisco. En esta zona se encuentran las corporaciones tecnológicas más grandes de Estados Unidos, así como también, múltiples nuevas empresas en tecnología llamadas *start-*

---

to Barack Obama, [col. Library of America], Nueva York, Penguin Random House, 2011, p. 233. [traducción propia]
[220] Complejo militar-industrial, ver término en el glosario.
[221] Dwight D. Eisenhower, "Farewell Address", *op.cit.,* p. 234. [traducción propia]
[222] *Ídem.*

ups.

Silicon Valley, cuya traducción literal es el Valle del Silicio, porta este nombre "por los creadores de los chips de silicio y las manufacturas que solían ensamblarlos ahí".[223] Sin embargo, Silicon Valley también se utiliza como concepto para designar al conjunto de empresas de la tecnología y de las comunicaciones de Estados Unidos.

En entrevista con *El País Semanal*, Evgeny Morozov, intelectual bielorruso experto en tecnología, argumentó que para entender a Silicon Valley "hay que mirar a Wall Street, al Pentágono, a las finanzas, a la geopolítica o al imperialismo".[224]

Si seguimos la línea de pensamiento de Evgeny Morosov, las empresas de las tecnologías de las comunicaciones, son determinantes en la geoestrategia[225] del país, o, para decirlo de otro modo, las empresas de las tecnologías de las comunicaciones ayudan a la gestión estratégica de los intereses geopolíticos.

2.3.3 Columna vertebral de internet en Estados Unidos

Lo que interesa en este apartado es analizar de qué manera las empresas de las comunicaciones, participan junto con el gobierno para estructurar el sistema de vigilancia que recientemente se ha llamado la industria de la vigilancia. Para llegar a este punto, analizaremos la relación con empresas tan antiguas como AT&T, pero también con las de creación reciente como lo son aquellas que se surgieron a partir de la invención de las redes sociales.

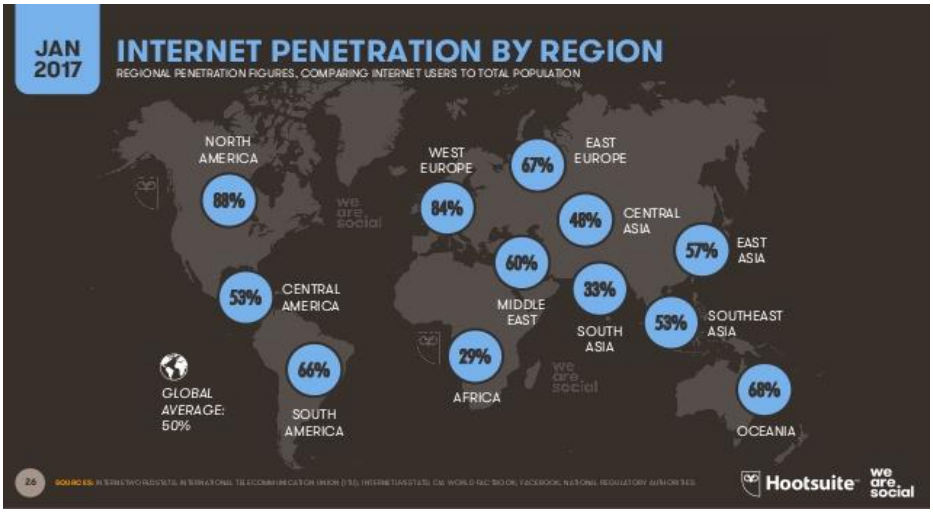
Primero, tenemos que entender que el sistema de vigilancia que conocemos en la actualidad, con sus alcances, no pudo ser posible en otro momento de la historia. Parte de lo que le permite ser masivo, son las capacidades técnicas, en concreto, en el espacio cibernético.

Para acceder al ciberespacio se necesita de la infraestructura para hacerlo, el cableado de cobre, las amplias redes de cable de fibra óptica, satélites, antenas terrestres, centros de almacenamiento de datos, etcétera. Los cables de fibra óptica están en su mayoría controlados por Estados Unidos. Los ISP, por sus siglas en inglés, son las compañías que transportan el tráfico de Internet; los "ISP nacionales, que poseen y operan miles de kilómetros de cable de

[223] "Silicon Valley", Techopedia: www.techopedia.com/definition/565/silicon-valley
[224] Joseba Elola, "Entrevista a Evgeny Morozov", El País Semanal: Las mil y un caras de la locura, Madrid, domingo 20 de diciembre de 2015, pp. 28-32.
[225] Geoestrategia se define en el glosario.

fibra óptica que recorren el país de un extremo a otro y conectan todas las grandes ciudades son: Verizon, AT&T, Qwest, Sprint, Level 3 y Global Crossing. (…)Sus grandes instalaciones de fibra óptica conforman la columna vertebral de Internet en Estados Unidos".[226]

¿Por qué al intervenir los cables de fibra óptica se obtiene una amplia cobertura de vigilancia y por lo tanto información? La principal razón radica en que a pesar de la existencia de los satélites, los cables de fibra óptica tienen un costo mucho menor y soportan grandes cantidades de datos, se podrían considerar la evolución del cable coaxial, por esta razón, "el 99% del tráfico de internet transcontinental viaja por estos cables […]".[227]Además, el uso de internet crece cada día. En la imagen siguiente se muestra el porcentaje de usuarios de del total de la población por región para enero de 2017.



Fuente: Simon Kemp, "Digital in 2017. Global Overview. A collection of Internet, social media and mobile data from around the world", We are social.[228]

La población mundial, según el "Panorama general. Informe sobre Desarrollo Humano 2015"[229] publicado por el Programa de las Naciones Unidas para el Desarrollo, PNUD, es de

[226]Richard A. Clarke, Robert K. Knake, Luis Alfonso Noriega (trad.), *Guerra en la red. Los nuevos campos de batalla*, *op. cit.,* p.109.

[227] Franz-Stefan Gady, "Undersea Cables: How Russia Targets the West's Soft Underbelly", The Diplomat. Read the Diplomat, Know the Asia-Pacifife, 27 de octubre de 2015, https://thediplomat.com/2015/10/undersea-cables-how-russia-targets-the-wests-soft-underbelly/ [traducción propia]

[228] Simon Kemp, "Digital in 2017. Global Overview. A collection of Internet, social media and mobile data from around the world", Special reports, We are social, 24 de enero de 2017, https://wearesocial.com/special-reports/digital-in-2017-global-overview

[229] Selim Jahan (director y autor principal), *Panorama general. Informe sobre Desarrollo Humano 2015. Trabajo al servicio*

7,300 millones de personas; para la Unesco, otro organismo de la ONU, en 2014 "más de 40% de la población mundial tiene ya acceso a Internet, cuyo número de usuarios habrá aumentado de 2, 300 millones en 2013 a 2, 900 millones a finales de 2014"[230], sin embargo para 2017, el número de personas con acceso a Internet en el mundo es de 4, 156, 932, 140[231] de usuarios. Las cifras hablan por sí mismas.

Aunado a esto, "La lengua de internet es el inglés, y una abrumadora proporción de las conversaciones globales a través del ordenador se origina también en los Estados Unidos, lo que influencia los contenidos de la conversación global".[232]

2.3.3.1 AT&T, Verizon y Sprint

Regresemos a las grandes compañías. AT&T es una de las compañías cuya infraestructura de cables de fibra óptica es crítica para el tráfico de internet tanto nacional como internacional. "Para interceptar los datos que transitan por esos cables, la NSA no sólo necesita tener control sobre una parte de las empresas que administran esas inmensas redes de telecomunicación, sino que también debe instalar dispositivos esenciales en su corazón".[233] Así lo hizo la NSA con AT&T.

Mark Klein, quien "hizo su carrera como especialista en fibra óptica en AT&T"[234], filtró a la opinión pública la existencia de una habitación en AT&T operada por la NSA, conocida como "el cuarto secreto". En el artículo "Una historia de la vigilancia" (*A story of Surveillance*) publicado por *The Washington Post* en noviembre de 2007, se documentaron los hallazgos de Klein. La NSA tiene ahí la función de recolectar todo el tráfico de internet que pasa por el cableado de AT& T, ¿cómo lo hace? A través de prismas de cristal que dividen las señales de cada red y crean dos copias iguales; una alimenta "el cuarto secreto" y la otra llega a

---

del desarrollo humano, Publicado por el Programa de las Naciones Unidas para el Desarrollo (PNUD), http://www.un.org/es/publications/publipl225.shtml

[230] s/a, "Medio mundo estará en línea en 2017", All News, Unesco, https://es.unesco.org/news/medio-mundo-estará-línea-2017

[231] s/a, "Internet usage statistics. The Internet big picture. World Internet Users and 2018 Population Stats", Miniwatts Marketing Group, https://www.Internetworldstats.com/stats.htm

[232] Zbigniew Brzezinski, *El gran tablero mundial. La supremacía estadunidense y sus imperativos geoestratégicos*, *op. cit.,* pp. 34 y 35.

[233] Antoine Lefébure, *El caso Snowden. Así espía Estados Unidos al mundo*, *op. cit.,* p. 163.

[234] *Ídem.*

su destino.

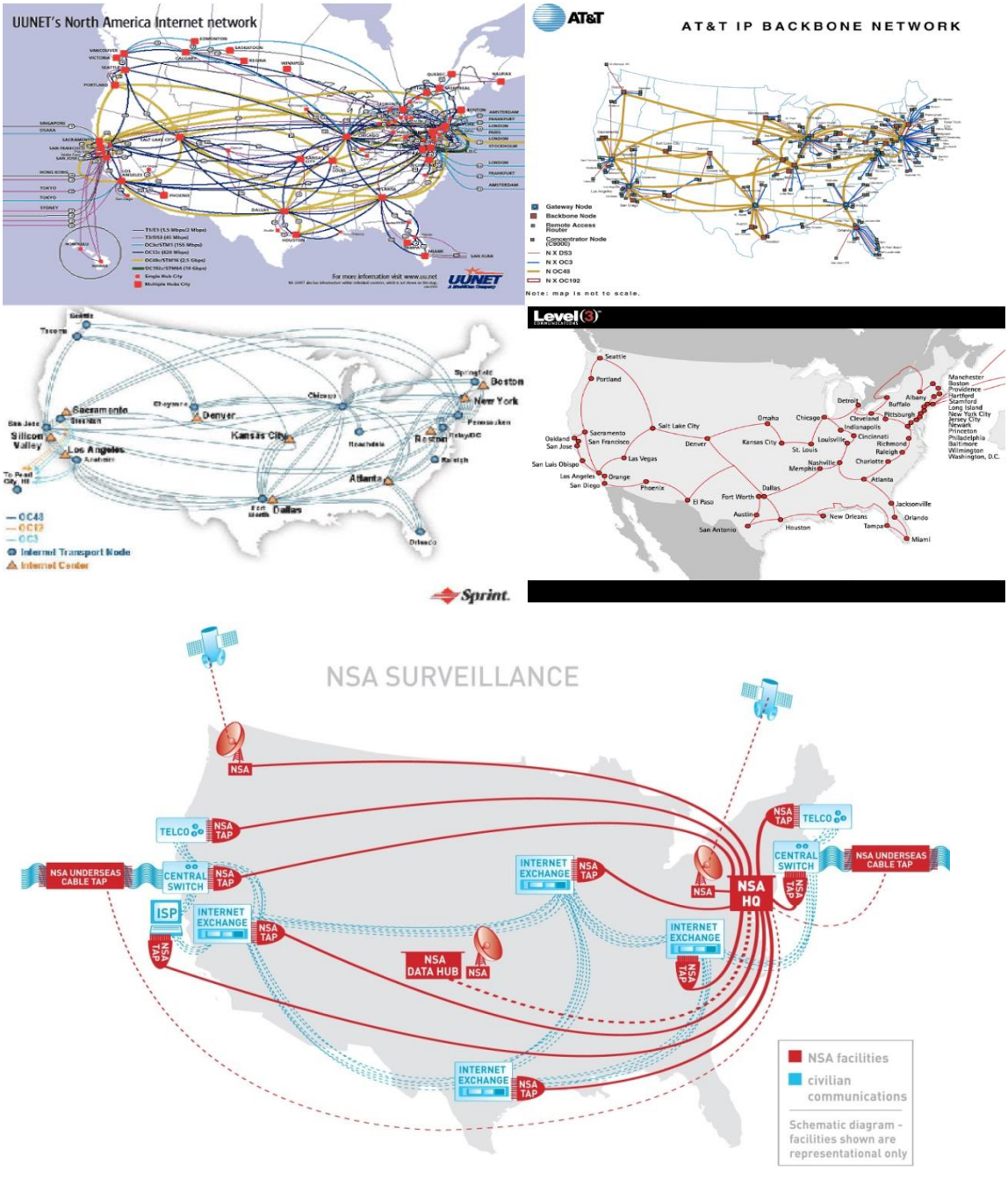
El artículo especifica la información de uno de los documentos en poder de Mark Klein, en el que aparecen los enlaces de varias compañías de las comunicaciones que comparten su información, "se incluye a Global Crossing, un proveedor de servicios de voz y data en Estados Unidos y el extranjero; UUNet, una gran compañía que provee internet en el Norte de Virginia adquirida por Verizon; Level 3 Communications, la cual provee transmisiones locales, de larga distancia y de data en Estados Unidos y el extranjero; y nombres más familiares como Sprint y Qwest. También incluye intercambio de data de MAE-West y PAIX conocida como Palo Alto Internet Exchange; instalaciones donde las compañías de telecomunicaciones que transportan el tráfico de internet se entregan la información una a la otra."[235]

Las empresas de las telecomunicaciones también reciben ganancias por su relación con el gobierno. La relación que tienen con la NSA no radica únicamente en principios que responden a su moral patriótica, la moral de los dólares también es factor determinante. En el artículo "A AT&T, Verizon y Sprint, la NSA les paga en efectivo por obtener tus comunicaciones privadas"(*AT&T, Verizon, Sprint are paid cash by NSA for your private communications)* publicado por la revista Forbes en 2013, se documentó en un reporte filtrado, escrito por el inspector general de la NSA, que fue publicado por *The Washington Post*, AP, y *The New York Review of Books*, que "la NSA mantiene relaciones con más de 100 compañías; Estados Unidos tiene la ventaja de ser el principal punto para las comunicaciones globales."[236] Además, la NSA le paga a AT&T, Verizon y Sprint cifras millonarias por acceder al 81% de las llamadas internacionales que entran a Estados Unidos. En efecto, "AT&T cobra $325 dólares por cuota de activación por cuenta y $10 dólares al día para monitorearla", "Verizon cobra $775 dólares por interceptar una cuenta el primer mes y después $500 dólares al mes, el artículo de AP reportó que Microsoft, Yahoo y Google se rehusaron a decir cuánto le cobraban al gobierno por permitir que interceptara correos electrónicos, y otras comunicaciones no telefónicas"[237]. Sin embargo, "la NSA le paga a las compañías de las telecomunicaciones 300 millones de dólares

[235] Ellen Nakashima, "A Story of Surveillance", Washington Post, 7 de noviembre de 2007, http://www.washingtonpost.com/wp-dyn/content/article/2007/11/07/AR2007110700006.html
[236] Robert Lenzner, "AT&T, Verizon, Sprint are paid cash by NSA for your private communications", Forbes, 23 de septiembre de 2013, http://www.forbes.com/sites/robertlenzner/2013/09/23/attverizonsprint-are-paid-cash-by-nsa-for-your-private-communications/#34d562341f15
[237] *Ídem.*

al año por obtener acceso a la información de sus comunicaciones".[238]

AT&T y Verizon son las dos compañías más poderosas de telecomunicaciones a nivel mundial en 2017, según el listado de la revista Forbes "Forbes Global 2000", e incluso superan a China Mobile que se encontraba a la cabeza de la lista en años pasados.



Fuente: American Civil Liberties Union, ACLU, "Eavesdropping 101: What can the NSA do?"

[238] *Ídem.*

No sólo sucede entre compañías de Estados Unidos y su complicidad con la NSA. El intercambio de información sucede también entre agencias gubernamentales como la NSA y la GCHQ, su aliada británica. El periódico *The Guardian* almacena y comparte una sección en línea dedicada a las filtraciones de Edward Snowden llamada "Los expedientes Snowden" *(The Snowden Files)*. Ahí, en el artículo titulado "La GCHQ interviene los cables de fibra óptica para acceder a las comunicaciones del mundo" (*GCHQ taps fibre-optic cables for secret acces to world's communications)*, se muestran dos de las secciones de la agencia: 1, el dominio de internet y 2, la explotación de las telecomunicaciones globales. *The Guardian* argumenta que el objetivo de estas secciones es "espiar el mayor tráfico de internet y de llamadas telefónicas que sean posibles" para "compartir la información con su socio estadunidense, la NSA".[239] Al tiempo de la publicación del artículo, en junio de 2013, se conocía la existencia de una operación cuyo nombre en código es Tempora, la cual llevaba en funciones dieciocho meses. Con la operación Tempora, la GCHQ puede "intervenir grandes volúmenes de data de los cables de fibra óptica y almacenarlos hasta por treinta días para que la información recolectada puede ser examinada con cuidado y analizada".[240]

Además, el artículo comparte que la GCHQ y la NSA "procesan grandes cantidades de información de personas inocentes así como de sospechosos"[241]; entre sus actividades se incluye "grabar llamadas telefónicas, el contenido de correos electrónicos, entradas de Facebook, y el historial de acceso a páginas de internet".[242]

Mientras que las grandes compañías privadas del cableado de fibra óptica recolectan toda la información posible, las agencias de espionaje se dedican a almacenarla y examinarla. Recordemos lo que dijo E. Morozov, tenemos que pensar en los grandes poderes si queremos entender a las compañías de las tecnologías de la información o *Silicon Valley*.

Los archivos que filtró Edward Snowden dan muestra de cómo operan estas agencias de Inteligencia con compañías de tecnologías de las comunicaciones, como se dijo en el noticiero *CNN breaking news* respecto a las primeras filtraciones del ex analista de la CIA:

---

[239] Ewen MacAskill, Julian Borger, Nick hopkins, Nick Davies y James Ball, "GCHQ taps fibre-optic cables for secret acces to world's communications", The Guardian, 21 de junio de 2013, http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa
[240] *Ídem.*
[241] *Ídem.*
[242] *Ídem.*

> "*The Washington Post* y *The Guardian* reportan que la Agencia Nacional de Seguridad, NSA y la Oficina Federal de Investigaciones, FBI, están recurriendo directamente a los servidores centrales de nueve compañías de Internet como Microsoft, Yahoo, Google, Facebook, AOL, Skype, Youtube y Apple. El informe dice que están extrayendo audio, video, fotografías, correos electrónicos, documentos y registros de conexión que permiten a los analistas rastrear las acciones de una persona y su contexto en el tiempo."[243]

2.4 Google

El número de usuarios que interactúa con alguno de los servicios (Google, Gmail, Youtube, Google Chrome, Google Maps, Google+, etcétera) de la trasnacional Alphabet Inc., cuya compañía principal es Google LLC, asciende a los 2.2 miles de millones de usuarios. Recordemos que hay más de 3 mil millones de usuarios de internet en el mundo, dos de las terceras partes de internautas globales usan alguno de sus servicios. En la era de la tecnología digital dichos datos, nos da una aproximación al vasto espectro de acción que tiene una empresa con tal cantidad de usuarios.

Según los datos oficiales de Google[244], hay 40, 000 personas trabajando para la compañía a los que ellos mismos denominan *Googlers*. Lary Page es el fundador y director ejecutivo del imperio informático, mientras que desde hace diez años Eric Schmidt funge como su presidente ejecutivo.[245] A su vez, Jared Cohen director del *think tank* Ideas de Google, sirvió como asesor para dos secretarías de Estado, con Condolezza Rice y con Hillary Clinton.

> Schmidt, delegado consejero de Google en 2001, estaba redactando un tratado en colaboración con Jared Cohen, director de Google Ideas, un departamento de Google que se describía y se describe a sí mismo como un 'comité interno de expertos teórico-prácticos'. […] Lo cierto es que en 2010 se había trasladado a Google desde el

[243] Laura Poitras, *Citizenfour*, Praxis Films, Participant Media, HBO Films, Estados Unidos, Alemania, 2014, 144 minutos.

[244] s/a, "The people behind Google", Google Company, www.google.com/about/company/facts/

[245] *Ídem.*

> Departamento de Estado de Estados Unidos, […] trabajó bajo dos administraciones distintas, un cortesano del mundo de la creación de ideas políticas, que llegó a ocupar el cargo de asesor en jefe de las secretarias de Estado Condoleezza Rize y Hillary Clinton.[246]

En mayo de 2011, el fundador y editor en jefe de WikiLeaks, Julian Assange, recibió la noticia que el presidente ejecutivo de Google, Eric Schmidt, buscaba una reunión con él para buscar asesoría en cuestiones tecnológicas relacionadas con la publicación de un libro. En junio del mismo año, tuvo lugar la reunión. A ésta asistieron además de Schmidt y Jared Cohen, Lisa Shields, vicepresidenta del Consejo de Relaciones Internacionales y "un tal Scott Malcomson, el editor del libro. Tres meses después de la reunión, Malcomson sería nombrado jefe de redactores de discursos en el Departamento de Estado y principal asesor de Susan Rice (entonces embajadora de Estados Unidos ante las Naciones Unidas y actualmente consejera de Seguridad Nacional); anteriormente había sido asesor en jefe en la ONU y durante muchos años ha sido miembro permanente del Consejo de Relaciones Internacionales". [247]

En el artículo "Bienvenidos al SplInternet" *(Welcome to the SplInternet)* publicado por *The World Post*, Scott Malcomson argumentó que internet fue posible gracias a la globalización y de que "Estados Unidos de manera desinteresada sostenía las llaves del ciberespacio en nombre del mundo entero"[248], llamándolo una hegemonía benigna. Malcomson, argumenta que los que no son estadunidenses "ya no confían en Estados Unidos lo suficiente para poner sus intereses nacionales a un lado en el caso de internet; tampoco quieren depender, para su propia prosperidad, e incluso seguridad, en el altruismo e independencia política de las compañías de tecnología estadunidenses[249]"; a su vez, el autor dice que en el caso de los estadunidenses, "no aceptan que la vida tecnológica del siglo XXI se obtiene al precio de la vulnerabilidad ante la vigilancia (…), recientes llamados a bloquear la publicación de terroristas en las redes sociales de parte de – Hillary Clinton, la Senadora Dianne Feinstein y Eric Schmidt– refleja una

[246]Julian Assange, Iván Barbeitos García (trad.), *Cuando Google encontró a WikiLeaks*, Ciudad Autónoma de Buenos Aires, Capital Intelectual, 2014, pp. 14 y 15.
[247] *Ibíd.,* pp. 28 y 29.
[248] Scott Malcomson, "Welcome to the SplInternet", The World Post, 21 de diciembre de 2015, http://www.huffingtonpost.com/scott-malcomson/welcome-to-the-splinterne_b_8855212.html [traducción propia]
[249] *Ídem.*

creciente convicción estadunidense en la que la responsabilidad del estado de proteger a sus ciudadanos se debe extender a restricciones del discurso cibernético"[250]. Esto nos da la perspectiva que tiene Google acerca de internet y la participación gubernamental.

En febrero de 2012, WikiLeaks empezó a publicar lo que se conocen como los Archivos de Inteligencia Global (*Global Intelligence Files*). Estos archivos contienen "cinco millones de correos electrónicos de las oficinas centrales en Texas de la compañía de 'Inteligencia global' Stratfor"[251]. En el documento filtrado y publicado el 14 de marzo de 2012 titulado "Re: Google e Irán **para uso interno solamente, favor de no reenviar**" (*Re:Google & Iran **internal use only-pls do not forward**)* escrito por Fred Burton, vicepresidente del Departamento de Inteligencia de Stratfor, se dijo que "Google obtiene apoyo y cobertura área de la Casa Blanca y del Departamento de Estado. En realidad (Google) hace cosas que la CIA no puede hacer. Va a hacer que lo secuestren o que lo maten; aunque para ser sincero, puede ser lo mejor para exponer el papel encubierto que desempeña Google a la hora de inflar levantamientos. Entonces el gobierno de Estados Unidos podrá decir que no tenía conocimiento y Google se quedará sosteniendo la bolsa de mierda".[252]

En el mismo archivo filtrado pero que corresponde a otro correo escrito por Jared Cohen y enviado a un ejecutivo de altos rangos de Google; el propio Cohen dijo que: "quiero su seguimiento y opiniones en el viaje propuesto para marzo en el que iré a los Emiratos Árabes Unidos, Azerbaiyán y Turquía. El propósito de este viaje es participar exclusivamente con la comunidad iraní en entender los retos que enfrentan los iraníes como parte de uno de nuestros grupos de Google Ideas especializados en sociedades represivas".[253]

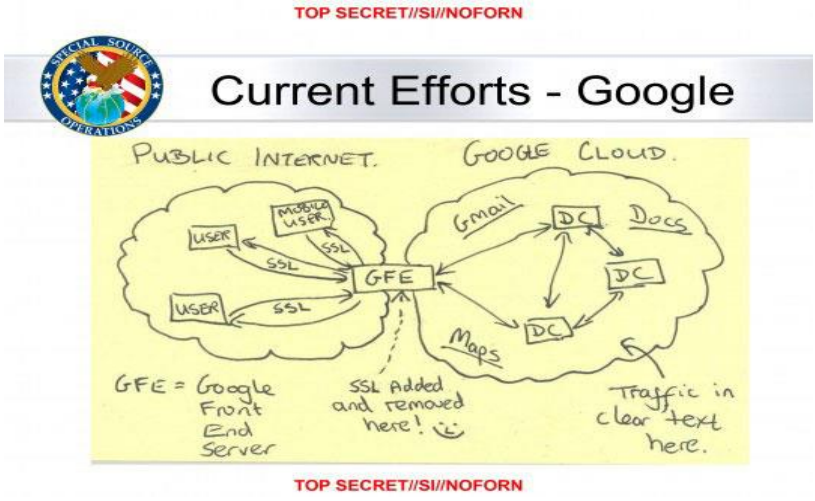
Otro ejemplo de la inclusión de Google en la política del gobierno de Estados Unidos se muestra en el archivo "Autorización del país otorgada para que Jared Cohen se reúna con el Secretario General Adjunto Bob Orr" (*Country clearance granted for Jared Cohen to meet with ASG Bob Orr)*. Este archivo, que pertenece a la sección de filtraciones de WikiLeaks "Biblioteca Pública de la Diplomacia Estadunidense", elaborado por las Naciones Unidas para

---

[250] *Ídem.*
[251] *The Global Intelligence Files,* WikiLeaks, search.WikiLeaks.org/gifiles/?viewemailid=1121800
[252] "*Re: Google & Iran **internal use only -pls do not forward**",* Email-ID 1121800, 2011-02-27, de: burton@strartfor.com, para: scott.stewart@stratfor.com, secure@stratfor.com, The GiFiles, WikiLeaks, search.WikiLeaks.org/gifiles/?viewemailid=1121800 [traducción propia]
[253] *Ídem.*

la Secretaría de Estado, contiene la siguiente información: "En respuesta a Refte, la ONU/Estados Unidos concede desde la Secretaría de Políticas de Planeación, autorización a Jared Cohen para reunirse con Robert C. Orr , asistente de la Secretaría General para la Coordinación Política y Planeación Estratégica [254], el 30 de mayo y darle continuidad a la colaboración para construir redes de víctimas del terrorismo".[255]

El entonces secretario de la defensa, Ash Carter, afirmó que Eric Schmidt, ex presidente ejecutivo de Google y actual director de Alphabet Inc, "encabezará la nueva junta consultiva del Pentágono, encargada de acercar las mejores prácticas e innovaciones de *Silicon Valley* al ejército de Estados Unidos"[256], la junta se llama: Junta Consultiva de Innovación para la Defensa (*Defense Innovation Advisory Board)*. De acuerdo a la opinión de Ash Carter, "la junta le dará al Pentágono acceso a las mentes más brillantes enfocadas en innovación tecnológica"[257]; de acuerdo a Scmidt "la junta ayudará a reducir la brecha entre la industria militar y la industria tecnológica.[258] En la siguiente dispositiva filtrada por Edward Snowden, se muestra el lugar de Google de donde obtiene los datos el gobierno de Estados Unidos.



Fuente: The Washington Post[259]

[254] El perfil de Robert C. Orr, se puede consultar en la página oficial de las Naciones Unidas o en la siguiente dirección electrónica: www.un.org/sg/management/senstaff_details.asp?smgID=134

[255] "Country Clearance Granted for Jared Cohen to meet with ASG BOB ORR", *Public Library of Us Diplomacy,* WikiLeaks, telegram (cable), Canonical ID: 08USUNNEWYORK489_a, 3 de junio de 2008, WikiLeaks.org/plusd/cables/08USUNNEWYORK489_a.htm

[256] Andrea Shalal, "Former Google CEO Schmidt to head new Pentagon innovation board", Reuters, 2 de marzo de 2016, http://www.reuters.com/article/us-usa-military-innovation-idUSKCN0W421V

[257] Andrea Shalal, "Former Google CEO Schmidt to head new Pentagon innovation board", *op.cit.*

[258] *Ídem.*

[259] Barton Gellman y Ashkan Soltani, "NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say", The Washington Post, 30 de noviembre de 2013 ,www.washingtonpost.com/world/national-security/nsa-infiltrates-

2.5 Las redes sociales

El diccionario Cambridge contempla dos definiciones para redes sociales, sin embargo, sólo una hace referencia al tipo de redes de las que nos ocupamos en este apartado. "Red social: página web o programa computacional que le permite a las personas comunicarse o compartir información vía internet a través de una computadora o teléfono celular."[260]La segunda definición es la base para comprender una red social, un grupo o grupos de personas que interactúan entre sí para comunicarse. Lo que interesa a estos individuos es la transmisión de información.

Empero, el uso de la información que transmiten estas redes varía, así como los actores que intervienen en ellas. Por ejemplo, en entrevista para *CNN* con Carmen Aristegui, el lingüista estadunidense Noam Chomsky, menciona el uso de la red social Facebook por parte de los gobiernos.

> Las compañías de medios estadunidenses que trabajan para Trump y Netanyahu […] en combinación con la oficina de Facebook en Berlín, actuaron en conjunto para crear un sistema en el que ellos pudiesen microdirigir a los electores alemanes. Facebook creo un perfil de toda la información masiva que tiene de individuos particulares. Tienen la información de millones de personas.
>
> Facebook en Berlín dividió a la población alemana en grupos que podrían ser influenciados por propaganda dirigida individualmente[…] que esta compañía de medios y Facebook hayan intervenido de esta forma y le hayan dado poder al partido fascista es real y es intervención estadunidense [en un proceso electoral externo].[261]

2.5.1 Facebook, Instagram y Whatsapp

La revista *Fortune* publica una lista anual de las quinientas empresas más lucrativas en Estados Unidos. "En total, las 500 compañías [que aparecen en la lista de] *Fortune*, representan dos

---

links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html?utm_term=.1318336f846d

[260] *Cambridge Dictionary,* en línea, entrada: "social network", https://dictionary.cambridge.org/es/diccionario/ingles/social-network [traducción propia]

[261] Carmen Aristegui, "Chomsky advierte sobre Google y Facebook", Aristegui, CNN, 21 de noviembre de 2017, https://www.youtube.com/watch?v=poJ5Q2tX0bU

tercios del producto interno bruto de Estados Unidos"[262]. Para tener una idea del poder económico de las compañías de las tecnologías de la información y las comunicaciones, en su edición de 2017, Apple se encuentra en tercer lugar, A& T en el noveno, Verizon en el catorceavo, Alphabet (Google), en el veintisieteavo y Facebook se ubica en el lugar noventa y ocho.

Facebook según la revista *Fortune*, al 31 de marzo de 2017, tenía un valor 410, 522 millones de dólares, 17, 048 empleados, aunque según las propias estadísticas de Facebook cuenta con 23, 165 empleados[263]. Facebook es dueña de Instagram, una red social en la que se comparten fotografías y en 2014 compró el servicio de mensajería instantánea Whatsapp.

Facebook reporta 1.37 miles de millones de usuarios al día y 2.07 miles de millones de usuarios al mes, según los datos propios de la empresa. Tiene oficinas internacionales en "Ámsterdam, Auckland, Berlín, Brasilia, Bruselas, Buenos Aires, Dubái, Dublín, Gurgaon [zona conurbada de Delhi, India], Hamburgo, Hong Kong, Hyderabad [también en la India], Yakarta, Johannesburgo, Karlsruhe [Alemania], Kuala Lumpur, Londres, Madrid, Melbourne, Ciudad de México, Milán, Montreal, Mumbai [Bombay, India], Nueva Delhi, París, San Paulo, Seúl, Singapur, Estocolmo, Sídney, Tel Aviv, Tokio, Toronto, Vancouver, y Varsovia"[264], además de trece oficinas en Estados Unidos.

Encima de la diversidad de puntos geográficos en los que Facebook cuenta con oficinas, lo interesante son los centros de datos que ha ido construyendo. "Cada centro de datos contiene miles de servidores computacionales conectados entre sí formando una red que se conecta al exterior a través de cables de fibra óptica".[265] En las imágenes siguientes, se muestran centros de datos de la compañía.

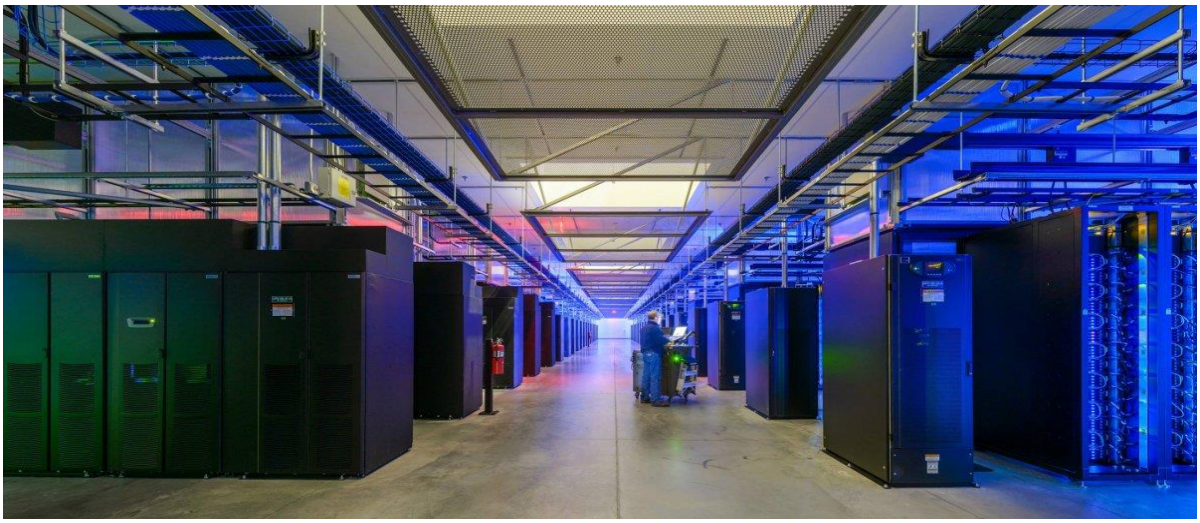
[262] Scott DeCarlo, "Fortune 500", Fortune, 2017, http://fortune.com/fortune500/
[263] s/a, "Stats", Company info, Newsroom, Facebook, https://newsroom.fb.com/company-info/
[264] *Ídem.*
[265] s/a, "The Facebook Data Center FAQ", Data Center Knowledge, http://www.datacenterknowledge.com/data-center-faqs/facebook-data-center-faq

Centro de datos de Facebook en Suecia

Fuente: *Business Insider*[266]

Centro de datos de Facebook en Prineville, Oregon

Fuente: *Business Insider* [267]



Sin especificar la locación. Fuente: *Business Insider*[268]

[266] *Ídem.*
[267] Dave Smith, "Take a look at Facebook´s gorgeous data centers from around the world", Business Insider, 16 de febrero de 2017, http://www.businessinsider.com/facebook-data-centers-photos-2017-2/#heres-a-look-inside-facebooks-data-center-in-forest-city-north-carolina-the-company-launched-this-center-in-2010-1
[268] *Ídem.*

2.6 Centros de datos

Un centro de datos necesita para funcionar grandes cantidades de energía traducida en electricidad; no sólo para las actividades que realizan los miles de servidores, dispositivos de almacenamiento y conexión a internet, es decir a los cables de fibra óptica, sino también para el enfriamiento que todo esto requiere. Por eso, no es de sorprender que muchos de ellos se encuentren instalados en lugares remotos con acceso a agua: ríos, lagos o presas. Por ejemplo, "[…] Google y otros titanes de *Silicon Valley* se acercan al río Columbia para abastecer ciclos incesantes de electricidad a un quinto del costo que tendría en el área de la Bahía de San Francisco"[269]. Además, cerca de ese río, se encuentra el nodo principal del cable de fibra óptica PC-1, este conecta Estados Unidos con Asia.

Pero más allá de los altos costos ambientales que tienen son fábricas de información. El fenómeno conocido como "la nube", no es más que la progresiva apropiación por parte de los centros de datos de funciones que antes realizaba una computadora convencional. Dentro de sus funciones se encuentran administrar los servicios de correo electrónico como Gmail por parte de Google o Hotmail por parte de Microsoft, la vinculación de todos los dispositivos de un usuario a una misma cuenta, fotografías como en el caso de Facebook, lugares de visita, mapas, libros guardados por el usuario, documentos de texto, notas, etcétera. En una palabra, información. "una de las reglas no dichas de la nueva carrera armamentista es que toda la información es estratégica".[270] Es la centralización de la tecnología informática, contrario a lo que se pensó que era internet. Mayor centralización se traduce en mayor control en menos manos.

[269] George Gilder, "The Information Factories", Wired, 10 de enero 2006, https://www.wired.com/2006/10/cloudware/ [traducción propia]
[270] *Ídem.*

3

Resistencias frente a la distopía

> "Los Estados y sus amigos asumieron el control de nuestro nuevo mundo [virtual] al controlar sus puntales físicos. El Estado, como un ejército que cerca un pozo petrolífero, o un agente de adunas que se deja sobornar, pronto aprendería a aprovechar el control físico que ejercía sobre el valioso espacio para introducirse en el reino platónico. Evitaría así la independencia que habíamos soñado, y luego, ocupando las líneas de fibra óptica y las estaciones terrestres de comunicaciones por satélite, continuaría interceptando masivamente el flujo de información de nuestro nuevo mundo, con lo que toda relación humana, económica y política pasaría a formar parte de una única e intricada red de redes mundial".[271]
>
> Julian Assange

3.1 Criptografía, una introducción

¿Qué es la criptografía? Para el diccionario de la Real Academia Española, es "el arte de escribir con clave secreta o de un modo enigmático".[272] En el diccionario Cambridge se le asignan dos definiciones; la primera, define a la criptografía como "la práctica de crear y entender códigos que mantengan la información secreta"[273], la segunda, se refiere a las computadoras y el "uso especial de códigos que mantengan la información segura en las redes digitales"[274].

Desde una perspectiva histórica, la criptografía surge "con la expansión de la escritura y el nacimiento de grandes imperios en constante lucha fronteriza […], la transmisión segura de información se convirtió en una prioridad creciente de gobiernos e individuos."[275] Hoy por hoy,

[271] Julian Assange, María Maestro (trad.), Cypherpunks. La libertad y el futuro de Internet, México, *op.cit.,* p. 20.
[272] *Diccionario de la Lengua Española,* Real Academia de la Lengua Española, en línea, entrada: "criptografía".
[273] *Cambridge Dictionary,* en línea, entrada: "cryptography".
[274] *Ídem.*
[275] Joan Gómez Urgellés Joan, *Matemáticos, espías y piratas informáticos. Codificación y criptografía*, [col. El mundo es matemático], España, Impresia Ibérica, National Geographic, 2012, p. 9.

en la era tecnológica digital, cifrar o encriptar[276] las comunicaciones se ha vuelto necesario tanto para los Estados, como para los individuos contra la vigilancia de los primeros. Sin embargo, no son pocos los eventos históricos de los que consta su uso. Para tener una apreciación mayor de lo que significa en la actualidad, y poder contextualizarla, se reproduce un breve repaso de su historicidad. El énfasis de su desarrollo se consagra en la guerra.

- En la guerra del Peloponeso (siglo V. a.e.c), los espartanos utilizaron métodos de encriptación para codificar sus mensajes. "El griego Herodoto, considerado padre de la historiografía […] en el Libro III de su magna *Historia"*[277] documentó la hazaña de Histeo al escribir un mensaje en la cabeza de un hombre rapado, esperó a que el cabello de aquel volviera a crecer, posteriormente lo envió a su destinatario. Otra anécdota de la misma guerra, consiste en un mensaje oculto en una tablilla a la que se le removió la cera, se escribió el mensaje y se volvió a cubrir con la misma para ocultar el contenido. "No es de extrañar que un pueblo guerrero por excelencia como los espartanos […] fueran pioneros en el desarrollo de la criptografía".[278] En esta misma guerra, "se hizo habitual el uso el uso de largas tiras de papel sobre las que, una vez enrolladas en un bastón *(escitala)*, se escribía el mensaje. El cifrado se basaba en la alteración del mensaje original mediante la inclusión de símbolos innecesarios que desaparecían al enrollar el mensaje en el bastón, […], si no se disponía de las dimensiones exactas de la escitala, al interceptor del mensaje le era muy difícil [descifrarlo]".[279]
- Cayo Julio César vivió del año 104 al 44 a.e.c. "En el siglo I [a.e.c]; apareció otro cifrado […], conocido con el nombre genérico de *código César* por ser esta figura histórica uno de sus más asiduos practicantes. El código César es uno de los más estudiados en el ámbito de la criptografía, [… ilustra] los principios de la aritmética modular,[280] uno de los pilares del estudio matemático de la escritura en clave."[281]

[276] La distinción de estos conceptos se explica en el glosario en la entrada: "cifrar".
[277] Joan Gómez Urgellés, *Matemáticos, espías y piratas informáticos. Codificación y criptografía, op. cit.,* p. 21.
[278] *Ibíd.*, p. 22.
[279] *Ídem.*
[280] La aritmética modular se explica con mayor precisión en el glosario.
[281] Joan Gómez Urgellés, *Matemáticos, espías y piratas informáticos. Codificación y criptografía, op. cit.,* p. 25.

- En el caso de las escrituras sagradas: la Biblia y el Corán, hay evidencia que muestra que algunas partes se encontraban cifradas. "[En el Antiguo Testamento] hay fragmentos del texto […] encriptados con un cifrado de sustitución llamado *atbash"*[282]. En lo que toca al Corán, "la naturaleza fragmentaria de los escritos originales estimuló el nacimiento de una rama de la teología dedicada a la datación exacta de las distintas revelaciones, […] los estudiosos del Corán se sirvieron, entre otras técnicas, del estudio de la frecuencia de aparición […]. Ésta y otras iniciativas relacionadas con el sentido detallado de los textos sagrados fueron el germen de la primera herramienta específica del criptoanálisis inventada por el hombre: el análisis de frecuencias. El primero en dejar constancia escrita de esta técnica revolucionaria fue un sabio nacido en Bagdad en el año 801, de nombre al-Kindi".[283]
- En el siglo XVI en Inglaterra, la criptografía jugó un papel clave en la trama para decapitar a la Reina de Escocia, María Estuardo [María I de Escocia]. "Las pruebas clave presentadas por el servicio de contraespionaje de la reina Isabel [I de Inglaterra], liderado por […] Lord Walsingham, eran una serie de cartas de María dirigidas a Babington. […] Las cartas […] estaban cifradas por un algoritmo que combinaba cifrado y codificación".[284] De las cartas se desprendía, supuestamente, el consentimiento de María para el asesinato de Isabel. "[…], el mejor criptoanalista de Isabel, Thomas Phelippes, conocía el método de análisis de frecuencias y pudo descifrar las cartas […] […] 'la conspiración Babington' no pudo sino lanzar una poderosa señal a los gobiernos y agentes de toda Europa: el algoritmo de sustitución convencional ya no era seguro."[285]
- Leon Battista Alberti, italiano renacentista, inventó en "1460 un sistema de encriptación que consistía en añadir al alfabeto cifrado convencional, un segundo [alfabeto]."[286] Con base en los cifrados polialfabéticos se inventó el disco de Alberti; mecanismo que superponía en ruedas giratorias varios alfabetos, y que se utilizó "en conflictos como la guerra de Secesión norteamericana"[287].

---

[282] *Ibíd.,* 37.
[283] *Ibíd.,* 37 y 38.
[284] *Ibíd.*, p.41.
[285] *Ibíd.,* p. 42.
[286] *Ibíd.,* p. 43.
[287] *Ibíd.,* p. 45.

- En el siglo XIX, el inventor británico Charles Babbage, partió de las matemáticas aplicadas a la tecnología para encontrar la solución de los cifrados polialfabéticos. "[…] sólo recientes revisiones de sus notas nos han permitido identificarle como el pionero en descifrar la clave polialfabética. […] en 1863, el oficial prusiano Friedrich Krasiski hizo público un método similar. […] Ambas búsquedas convergían hacia un mismo punto y dieron luz a un mismo proceso: la mecanización".[288]

3.1.1 Guerras mundiales

3.1.1.1 Primera Guerra Mundial

De vuelta a lo que conocemos como historia reciente, después de una breve enumeración de eventos en los que participó la criptografía en la historia antigua; el telegrama Zimmerman es uno de los casos más conocidos de su uso e impacto en las relaciones internacionales. El nombre proviene del "[…] ministro de Exteriores [de Alemania], Arthur Zimmerman",[289] en el contexto de la Primera Guerra Mundial.

A principios del siglo XX ya existía una amplia red de cables telegráficos submarinos y continentales. Para Estados Unidos, "en 1844 se llevó a cabo la primera transmisión [telegráfica] y poco después se formó una compañía con el expreso objetivo de cubrir la totalidad de América del Norte con líneas telegráficas"[290], los telegramas se transmitían a través de un lenguaje electrónico codificado, llamado comúnmente Código Morse; "[…] éste es, en cierto modo, una primera versión de los futuros sistemas de comunicaciones digitales".[291]

En el momento que se emite el famoso telegrama, en 1917, ya había sucedido el hundimiento del barco británico Lusitania por submarinos alemanes. En el telegrama el referido el ministro alemán de Exteriores, A. Zimmerman, le proponía al presidente de México, Venustiano Carranza, establecer una alianza entre ambos países a cambio de devolverle a nuestro país los territorios de Nuevo México, Texas y Arizona. Asimismo, le hacía saber que la guerra submarina era inminente, así como la entrada de Estados Unidos a la guerra. El telegrama fue interceptado y descifrado por los británicos.

---

[288] *Ibíd.,* p. 51.
[289] *Ibíd.,* p. 15.
[290] *Ibíd.,* p. 53.
[291] *Ibíd.,* p. 56.

El Código Morse se utilizó para traducir los impulsos electrónicos a un lenguaje, y era de uso general. Para el uso de comunicaciones seguras, en un contexto de guerra, se necesitó encriptar los mensajes. "El gobierno británico […] desde poco después del inicio del conflicto había bloqueado los cables telegráficos submarinos que conectaban Alemania con el hemisferio occidental, de modo que toda comunicación eléctrica tenía que circular por cables susceptibles de ser interceptados por los ingleses. […] El gobierno británico interceptó el mensaje y lo remitió *ipso facto* a su departamento de criptoanálisis, conocido como Habitación 40".[292]

La cifra ADFGVX "es uno de los métodos más sofisticados de la criptografía clásica [sin máquinas]; introducido por los alemanes en 1918"[293] y descifrada por los franceses en la "Oficina Central de Cifras [donde] trabajaba un talentoso criptoanalista de nombre Georges Painvin".[294] El uso de cifrados por parte de los alemanes en la Primera Guerra Mundial, dejó ver la importancia que le asignaban los países al uso de comunicaciones seguras para la estrategia militar.

Las contrapartes daban la misma importancia a descifrar los códigos y analizarlos que a cifrar sus comunicaciones. De la Primera Guerra Mundial a la Segunda, se dio un gran salto en esta materia; el uso de máquinas para encriptar colocó un nuevo nivel de dificultad para descifrar las comunicaciones y otorgó mayor seguridad para su transmisión.

3.1.1.2 Segunda Guerra Mundial

Los casos más conocido del uso de máquinas para encriptar las comunicaciones en la Segunda Guerra Mundial fueron los de Enigma y Colossus. El primero, inventado por los alemanes, el segundo, por los gobiernos de Polonia y Gran Bretaña para descifrar el funcionamiento del primero. "En el año 1923, el ingeniero alemán Arthur Scherbius patentó una máquina diseñada para facilitar las comunicaciones seguras, […] Enigma"[295], "[… en] la historia del descifrado de Enigma […] intervinieron, sobre todo, los departamentos de Inteligencia de Polonia y Reino Unido, y tiene entre sus héroes al matemático […] Alan Turing, el hombre que es considerado

[292] *Ibíd.,* pp. 16 y 18.
[293] *Ibíd.,* pp. 57.
[294] *Ídem.*
[295] Joan Gómez Urgellés, *Matemáticos, espías y piratas informáticos. Codificación y criptografía, op.cit.,* p.60.

el padre de la moderna computación"[296] e inventor de Colossus.

Sin embargo, y sin afán de restar mérito alguno a Alan Turing, en el imaginario de la cultura popular de la historia moderna se considera a éste como el criptoanalista que encuentra el código para descifrar Enigma. Aunque en realidad Turing y su equipo construyen la máquina que será capaz de descifrar las comunicaciones encriptadas del ejército del Reich. Además, no se toma en cuenta el antecedente inmediato: "[…] el departamento de Criptoanálisis polaco, conocido como *Byuro Szyfrów*"[297], el cual tuvo acceso a máquinas Enigma, "[…] decidió incorporar [a su] equipo de analistas a un número considerable de matemáticos. Entre ellos a […] un joven de 23 años llamado Marian Rejewski".[298]

El mayor logro de este joven matemático fue reducir, de manera más que considerable, el número de claves que era capaz de brindar una máquina Enigma, de "diez mil billones iniciales a […] 105, 456"[299]. Para lograrlo, "[…] Reyewski logró construir un artefacto de funcionamiento similar a Enigma, conocido como *Bomba*, capaz de cotejar cualquiera de las posibles posiciones de los tres rotores [Enigma funcionó con base en un sistema de rotores que hacía posible maquinizar los cifrados] en busca de la clave diaria. En fechas tan tempranas como 1934, el *Byuro Szyfrów* había conseguido romper Enigma y era capaz de descifrar cualquier mensaje en un plazo de 24 horas".[300]

Las primeras constancias del uso de Enigma datan de la guerra civil española, "para las comunicaciones de mayor nivel, el bando nacional, liderado por el general [Francisco] Franco, disponía de […] treinta máquinas de las denominadas Enigma, suministradas por el Reich".[301] Por su parte, el lado republicano utilizó cifrados de sustitución que fueron fácilmente descifrados por los nacionalistas.

Aunque para 1934 el *Byuro Szyfrów* ya había descifrado la primera versión de Enigma, los alemanes le hicieron ajustes técnicos al sumarle rotores y clavijeros que aumentaron el número de claves posibles "[…] a cerca de 159 trillones. […] Aunque sabía cómo descifrar el código, el *Byuro Szyfrów* carecía de los medios necesarios para analizar secuencialmente un

---

296 *Ibíd.,* p. 61.
297 *Ibíd.,* p. 68.
298 *Ídem.*
299 *Ídem.*
300 *Ídem.*
301 Joan Gómez Urgellés, *Matemáticos, espías y piratas informáticos. Codificación y criptografía, op. cit.,* p. 63.

número 10 veces mayor [...]"[302]. "En 1939, con el conflicto ya desatado en el corazón de Europa y su país conquistado, los polacos remitieron sus máquinas Enigma y toda su información a sus aliados británicos"[303].

Ya con la información brindada por los polacos y las máquinas en su poder, el gobierno británico concentró su unidad de criptoanálisis "[…] en las afueras de Londres, en una hacienda llamada Bletchey Park"[304]. Alan Turing formó parte de este equipo e "ideó un sistema eléctrico que permitió reproducir todas y cada una de las 1, 054, 650 combinaciones posibles de orden y posición de los tres rotores en un tiempo inferior a 5 horas"[305]. Fue, en este contexto, donde "el equipo de Bletchey Park terminó por desarrollar el primer prototipo de ordenador moderno, bautizado como *Colossus."*[306] La era de las computadoras nacía.

3.2 Criptopunks

En 1981, el periódico ***uno****más****uno*** publicó, en su sección de información científica, un artículo intitulado "El uso de códigos secretos y el derecho a la privacía".[307] En éste ya se hace referencia al uso de la criptografía para defender la privacidad de los ciudadanos. Advierte, por ejemplo, de bancos de datos comunes, lo que hoy es parte de lo que conocemos como data, a los que entonces ya se tenía acceso, "los bancos de datos comunes -seguros, inversiones, registro de la propiedad, créditos, seguro social, censos, datos de empleo, registros académicos, etc.- permiten atisbar los detalles más íntimos de nuestras vidas y es prácticamente imposible saber quién se está enterando y con qué fines. Los bancos de datos pueden revelar desde el domicilio y el teléfono hasta la religión, el salario, calificaciones, confiabilidad como sujeto de crédito, la afiliación política, estado de salud, suscripciones a revistas y periódicos, los nombres de los miembros de la familia y de los amigos y aun las opiniones de diversas personas sobre la personalidad y desempeño profesional".[308]

Se sabía mucho de lo que hoy se sabe, la recolección de cientos de datos privados de los ciudadanos y la criptografía como medio de defensa ciudadana contra la intromisión. Sin

---

[302] *Ibíd.,* p. 68.
[303] *Ibíd.*, p. 69.
[304] *Ídem.*
[305] Joan Gómez Urgellés, *Matemáticos, espías y piratas informáticos. Codificación y criptografía, op.cit.,* p. 70.
[306] *Ibíd.,* p.71
[307] Víctor Miguel Lozano, "El uso de códigos secretos y el derecho a la privacia", *op.cit.*
[308] *Ídem.*

embargo, desde entonces, "el uso de códigos en clave podría mantener toda esta información segura y libre de toda interferencia. Por esta razón, y debido a que los códigos modernos poseen un gran interés teórico como problemas matemáticos, muchos científicos están interesados en la criptografía. Estos investigadores enfrentan, en Estados Unidos, la creciente oposición de la *National Security Agency* (NSA), el departamento del gobierno federal encargado de proteger los secretos gubernamentales y obtener información secreta de otros países".[309]

Fue tanta la influencia de esa Agencia en su determinación de evitar las investigaciones académicas sobre criptografía, que "se integró un comité con representantes académicos de la NSA, denominado Grupo para el Estudio Público de la Criptografía (PCSG, por sus siglas en inglés), con el fin de entablar un diálogo entre la NSA y la comunidad académica interesada en estudios criptográficos. Las cosas han sido conducidas de tal manera, que […] el PCSG recomendó una serie de procedimientos que darían poder a la NSA para cambiar u omitir porciones de artículos científicos que dicha Agencia considere como potencialmente lesivos o importantes para la seguridad de Estados Unidos."[310]

Sin embargo, hubo respuesta. En los años noventa del siglo XX tuvieron lugar las primeras criptoguerras: "[…] los activistas del movimiento criptopunk empezaron a difundir importantes herramientas criptográficas como *software libre*[311], y la administración federal de Estados Unidos buscó impedir su uso. Clasificó a la criptografía como munición y restringió su exportación; trató de introducir tecnologías rivales, que fueron deliberadamente quebrantadas para que las fuerzas de seguridad pudieran desencriptar sus contenidos, y también trató de introducir el controvertido plan –de custodia de claves—. […] en la actualidad se libra una segunda criptoguerra con esfuerzos técnicos y legislativos para relegar o marginar el uso de la criptografía".[312]

¿Qué propone el movimiento criptopunk?, ¿qué concepción tiene del poder?, ¿por qué se considera una alternativa a la vigilancia? El propósito de la sección dedicada a la criptografía fue que observáramos el papel que ha jugado en el cifrado y descifrado de las comunicaciones

[309] *Ídem.*
[310] *Ídem.*
[311] Software libre, ver el término en el glosario.
[312] "Nota al pie de página, no. 41" en, Julian Assange, *CYPHERPUNKS. La libertad y el futuro de internet, op.cit.,* pp. 60 y 61.

a lo largo de la historia, para así tener las bases para analizar su actual significado. El uso masivo de internet en la economía, la política y la creciente dificultad de mantener las comunicaciones en la esfera privada nos obligan a mirar las opciones. ¿La criptografía es una de éstas?

Como se advirtió en el primer capítulo, existen redes de vigilancia conformadas por grupos de países. Éstos, los dueños de la vigilancia, emplean la dicotomía discursiva Seguridad *vs.* Vigilancia para mantener las intervenciones de las comunicaciones de sus propios ciudadanos e imponen modelos de vigilancia a otros. El factor del capital privado es clave en la vigilancia, "[…] las empresas que venden costosos dispositivos gozan de lazos cercanos con los servicios de Inteligencia estadunidenses. Sus directores y empleados de confianza son matemáticos e ingenieros de la NSA, y capitalizan los inventos que han creado para la vigilancia de Estado"[313]. Entonces, ni los ciudadanos, ni los Estados que están fuera de la capacidad para crear su propia tecnología pueden asegurar que no son vigilados.

Los criptopunks "[…] buscábamos proteger la libertad individual de la tiranía del Estado, y la criptografía era nuestra arma secreta. Esto era subversivo porque la criptografía era entonces propiedad exclusiva de los Estados, utilizada como arma en distintas guerras. Al escribir nuestro propio *software* en contra de las superpotencias y extenderlo a lo largo y ancho del planeta, liberamos a la criptografía y la democratizamos. Esta fue una lucha realmente revolucionaria desarrollada en las fronteras del nuevo internet".[314]

3.2.1 Los manifiestos

Para la Real Academia de la Lengua Española, un manifiesto es un "escrito en que se hace pública declaración de doctrinas, propósitos o programas".[315] El movimiento criptopunk tiene sus documentos fundacionales, también la línea de pensamiento que seguirán aquellos que se inserten en este sistema de creencias y acciones. Se abordará la carta de Phil Zimmermann, el manifiesto criptoanarquista y el manifiesto criptopunk. Los tres documentos surgieron a principios de la década de los noventa del siglo XX.

[313] *Ibíd.,* p. 14.
[314] *Ibíd.,* p. 16.
[315] *Diccionario de la lengua española,* Real Academia de la Lengua Española, en línea, entrada: "manifiesto".

3.2.1.1 La carta de Phil Zimmermann

Phil Zimmermann, "físico estadunidense y activista en pro de la privacidad, ofreció de forma gratuita el sistema PGP (siglas del inglés *Pretty Good Privacy:* Privacidad razonable), un algoritmo de encriptación[316] capaz de funcionar en ordenadores domésticos."[317] Esto fue un gran salto hacia la criptografía de código abierto, aquella que el gobierno no controlaba. De esta manera, con la descarga de este programa, los usuarios obtenían sin costo alguno un programa de llave o clave pública[318]. De tal manera, podían encriptar sus comunicaciones sin correr el peligro de que fueran leídas por alguien no deseado. La distribución del sistema PGP fue acompañada por una carta del autor.

Fragmento de la carta Zimmermann

> […] No hay nada de malo en mantener tu privacidad. La privacidad es uno de los derechos que establece la Constitución [de Estados Unidos] (…) Nos movemos hacia un futuro en el que la nación será atravesada por redes de datos compuestas por cable de fibra óptica de alta capacidad, uniendo conjuntamente todos nuestros, cada vez más, omnipresentes ordenadores personales. El correo electrónico será lo normal, no la novedad como lo es hoy en día. El gobierno protegerá nuestros correos electrónicos con protocolos de encriptación designados por él mismo. Probablemente la mayoría de la gente esté de acuerdo con esto. Pero quizás algunos preferirían sus propias medidas de protección. (…) Si la privacidad está fuera de la ley, sólo los que están fuera de la ley tendrán privacidad. Las agencias de Inteligencia tienen acceso a una buena tecnología criptográfica. Así como los grandes traficantes de armas o de drogas. También los contratistas de defensa, las compañías petrolíferas y otras corporaciones gigantes. Pero la mayoría de la gente corriente, y de las organizaciones políticas de oposición, no tenían acceso a tecnología criptográfica militar de clave pública. Hasta ahora.
>
> El PGP permite a la gente tener su privacidad en sus propias manos. Hay una creciente

[316] Algoritmo de encriptación, ver entrada en el glosario.
[317] Joan Gómez Urgellés, *Matemáticos, espías y piratas informáticos. Codificación y criptografía, op.cit.,* p. 107.
[318] Llave pública, consultar entrada en el glosario.

necesidad social de privacidad. Por eso lo escribí.[319]

Es pertinente notar la manera en que Phil Zimmermann justifica haber escrito el sistema PGP. Desde su mirada de físico e informático, el uso de la criptografía en las comunicaciones electrónicas ya era común para las agencias de espionaje, traficantes, compañías petrolíferas y dueños del capital; por el otro lado están los ciudadanos con sus comunicaciones por completo desprotegidas. Por eso nace PGP y tiene éxito inmediato. En cuanto lo sube a internet, "se disemina en el viento como miles de semillas de diente de león"[320], "en horas se descargaba por todo el país [Estados Unidos] y más allá. [Phil Zimmermann afirmó que PGP] se encontraba en el extranjero el día después de liberarlo. 'Recibí correos electrónicos de casi todos los países de la tierra'"[321].

3.2.1.2 El Manifiesto Criptoanárquico

Tim C. May, ingeniero electrónico interesado en la criptografía, leyó en septiembre de 1992, en la reunión fundacional de los Criptopunks físicos *(Physical Cypherpunks)*, el manifiesto de los criptoanarquistas. Ahí se plasmaron líneas de acción y de pensamiento de aquellos que se consideran criptopunks.

La proclama comienza con una paráfrasis del Manifiesto Comunista de Carlos Marx: "Un fantasma recorre el mundo moderno, el fantasma de la criptografía anárquica".[322] Así como el Manifiesto de Carlos Marx declaró, en el siglo XIX, un paradigma nuevo de pensamiento que incitaba a romper con el modo de producción capitalista, el manifiesto criptoanarquista, propuso una nueva manera de concebir la comunicación electrónica.

Para Tim C. May, el anonimato que puede brindar la tecnología de la computación "[…] cambiará por completo la regulación gubernamental, la habilidad para imponer impuestos y controlar las interacciones económicas, la habilidad para mantener la información secreta, e incluso alterará la naturaleza de la confianza y la reputación".[323]

---

[319] Joan Gómez Urgellés, *Matemáticos, espías y piratas informáticos. Codificación y criptografía, op.cit.,* pp. 107 y 108.
[320] Steven Levy, "Crypto Rebel", Wired, 2 enero de 1993, https://www.wired.com/1993/02/crypto-rebels/ [traducción propia]
[321] *Ídem.*
[322] Tim C. May, *The Crypto Anarchist Manifiesto*, activism.net/cypherpunk/[traducción propia]
[323] *Ídem.*

La NSA no era ajena al movimiento criptopunk, ni a sus reuniones. El propio Tim C. May, en el manifiesto, aclara que los métodos de encriptación ya se conocían desde los años ochenta, "[aunque éstos…] se concentraron en conferencias académicas en Europa y Estados Unidos, conferencias monitoreadas de cerca por la NSA".[324] En la misma dirección que Phil Zimmerman, Tim C. May, reconoce que el uso de tecnología para encriptar las comunicaciones llega a diferentes ámbitos, "el Estado, por supuesto que tratará de atrasar o detener la difusión de esta tecnología; dirán que es por causas de Seguridad Nacional, el uso de esto por traficantes de drogas, evasores de impuestos y temores de desintegración social. Muchas de sus preocupaciones serán válidas; […] Criminales y elementos extranjeros serán usuarios activos de CryptoNet., pero esto no parará la diseminación de la criptoanarquía".[325]

Tim C. May también planteó el problema de la propiedad intelectual. Según él, como advirtió mediante una interesante metáfora, la criptoanarquía romperá los alambres de púas que la protegen.

3.2.1.3 El Manifiesto Criptopunk

En marzo de 1993, el matemático y programador estadunidense Eric Hughes publicó el Manifiesto Criptopunk. En éste se plantean los supuestos éticos que enarbolará el movimiento. Hughes aborda, en primer lugar, la diferencia entre privacidad y secrecía. Para él, una sociedad abierta en la edad electrónica necesita de la privacidad. Misma que explica como "el poder de revelarse uno mismo al mundo con selectividad"[326], mientras que la secrecía se explica como "algo que no quieres que nadie conozca".[327]

Sin embargo, hay otros factores relacionados con la privacidad: la libertad de expresión y la libertad económica. En este primer momento de los criptopunks, el poder de las comunicaciones electrónicas potencia las discusiones en grupo para crear conocimiento, así como la imperante necesidad de transacciones económicas privadas. Para lograrlo, proponen la criptografía como método, al subrayar que "la privacidad en una sociedad abierta […] requiere de la criptografía. Si digo algo, quiero que sólo se escuche por aquellos a los que va

[324] *Ídem.*
[325] *Ídem.*
[326] Eric Hughes, *A Cypherpunk's Manifesto*, Electronic Frontier Foundation, 9 de marzo de 1993, https://w2.eff.org/Privacy/Crypto/Crypto_misc/cypherpunk.manifesto [traducción propia]
[327] *Ídem.*

dirigido"[328]. En esta misma lógica desarrollan el aspecto económico: Si compro algo, quiero que sólo se entere de ello a quien hice la compra, e incluso ni éste tendría porqué conocer mi identidad.

Los argumentos son de carácter político y ético. Este manifiesto va dirigido a las grandes empresas y a los gobiernos poderosos. Los criptopunks definen, desde ese momento, a sus enemigos en la lucha.

> […] No podemos esperar que los gobiernos, las corporaciones y otras organizaciones sin cara, nos concedan la privacidad por cualidades benévolas. Es para su beneficio hablar de nosotros, y debemos esperar que lo hagan. Tratar de prevenir su discurso es pelear contra las realidades informativas. La información no sólo quiere ser libre, anhela la libertad. […] Debemos defender nuestra privacidad si es que esperamos tener alguna. Debemos de estar juntos y crear sistemas que permitan transacciones anónimas. La humanidad ha defendido su privacidad por siglos, lo ha hecho con susurros, oscuridad, sobres y cartas, puertas cerradas, saludos secretos y mensajeros. Las tecnologías del pasado no permitieron una privacidad fuerte, las tecnologías electrónicas lo permiten. […] Nosotros, los critptopunks, estamos dedicados a construir sistemas anónimos. Defendemos nuestra privacidad con criptografía.[329]

El movimiento de los criptopunks había iniciado.

3.2.2 Conversaciones entre criptopunks

Los planteamientos de los criptopunks, desde sus inicios, estuvieron encaminados a defender la libertad a la información y al uso de comunicaciones seguras. Sin embargo, la última generación llevó las cosas un nivel más adelante. Este apartado está dedicado a la conversación entre cinco criptopunks, donde exponen sus opiniones acerca de diversos asuntos como la privacidad, la libertad, la censura, la geopolítica y el poder. Después de todo, para los criptopunks "la criptografía puede proteger no sólo las libertades civiles de los individuos, sino también la soberanía e independencia de países enteros, la solidaridad entre grupos con causas

[328] *Ídem.*
[329] *Ídem.*

comunes y el proyecto de emancipación global."[330]

El debate se dio en junio de 2012 en el programa de Julian Assange, *The World Tomorrow, Cypherpunks* [331], en el canal de noticias RT. Los participantes fueron:

- "Julian Assange, uno de los máximos exponentes de la filosofía criptopunk en el mundo. Su trabajo con WikiLeaks ha dado una dimensión política a la tradicional yuxtaposición criptopunk: 'Privacidad para el débil, transparencia para el poderoso.' […] Julian es […] autor de numerosos proyectos de *software* acordes con la filosofía criptopunk, como *Strobe,* el primer escáner de puertos TCP/IP, el programa de encriptación *Rubberhorse,* y el código original para WikiLeaks.
- "Jacob Appelbaum es el fundador de Noisebridge en San Francisco, miembro del Club Berlinés del Caos Informático y desarrollador. Es, asimismo, uno de los principales defensores e investigadores del Proyecto Tor, un sistema de anonimato virtual creado para que todo el mundo pueda evitar la vigilancia y sortear la censura de internet.
- "Andy Müller-Maguhn fue uno de los primeros miembros del Club del Caos Informático en Alemania. […] Es uno de los cofundadores del EDRI (European Digital Rights/Derechos Digitales Europeos), una ONG pro derechos humanos de la era digital. […] especialista en telecomunicaciones y otros sistemas de vigilancia, trabaja como periodista en la industria de la vigilancia con su proyecto wiki[332], buggedplanet.info. Andy trabaja en comunicación criptográfica y fundó, con otros compañeros, una empresa llamada Cryptophone, que comercializa dispositivos seguros de comunicación de voz y ofrece asesoría estratégica en el contexto de la arquitectura de red.
- "Jeremie Zimmermann es cofundador y portavoz del grupo civil de apoyo La Quadrature du Net, la organización europea más destacada en el ejercicio de la defensa del derecho del anonimato en la red y en la concientización acerca de la existencia de ataques normativos a las libertades virtuales. […] en el Parlamento Europeo, su grupo, La Quadrature du Net, consiguió un hito histórico al dirigir exitosamente una campaña

[330] *Ibíd.,* p. 14.
[331] Julian Assange, "Cypherpunks" parte 1 y 2, *The Julian Assange Show*, Russia Today, 5 de junio del 2012, https://www.youtube.com/watch?v=eil_1j72LOA
[332] Consultar la entrada wiki en el glosario.

pública de rechazo a ACTA (Anti-Counterfeiting Trade Agreement/Acuerdo Comercial de la Lucha Contra la Falsificación).”[333]

Los ejes del análisis fueron los siguientes:

a) Mayor comunicación vs. Mayor vigilancia

> Ahora contamos con mayores comunicaciones frente a una mayor vigilancia. Mayor comunicación quiere decir que todos tenemos un plus de libertad con respecto a aquellos que intentan controlar las ideas y fabricar el consenso, y mayor vigilancia significa justamente lo contrario.[334] La vigilancia es, al día de hoy, mucho más evidente que la vigilancia del pasado, y la ejercen en bloque los estadunidenses, los británicos, los rusos y otros gobiernos (contados) como el sueco y el francés.[335]

El eje central del análisis en este tópico, pone sobre la mesa la situación del control de las comunicaciones. Por un lado, tenemos al Estado que, junto con el sector privado, crean las circunstancias para que exista mayor vigilancia y control a particulares. Por el otro, tenemos la oportunidad, como colectividad e individuos, de acceder a mayor información a través del aumento en la capacidad de las comunicaciones. Tanto una como la otra, mayor comunicación y mayor vigilancia, se traducen en mayor poder político, la pregunta es: ¿Hacia dónde se inclina la balanza? La respuesta de los Estados es volver los procesos técnicos incomprensibles a la mayoría de la humanidad, “[…] ese es el objetivo de este tipo de trabajo de Inteligencia, ralentizar un proceso quitándole a la gente la capacidad de entenderlo. Declarar algo en secreto significa que limitas la cantidad de gente enterada, es decir, la que conoce eso, y, por ende, la capacidad de afectar al proceso mismo”.[336]

Sin embargo, si existen las circunstancias políticas y sociales adecuadas puede lograrse una mayor comunicación que, traducida en consenso, dé pie a la actuación de las sociedades. Por ejemplo, en 2008 el pueblo egipcio salió a las calles a exigir la renuncia del presidente

[333] Julian Assange, María Maestro (trad.), *Cypherpunks. La libertad y el futuro de internet*, *op.cit.,* pp. 25-28.
[334] *Ibíd.,* p.39.
[335] *Ídem.*
[336] Andy Müller-Maguhn en, Julian Assange, María Maestro (trad.), *Cypherpunks. La libertad y el futuro de internet*, *op.cit* p. 41.

Mubarak. Mubarak, quien, temeroso del diálogo libre que posibilitaba internet suspendió, precisamente, "[…] el acceso a internet en Egipto. […] la gente se vio obligada a salir a la calle para enterarse de lo que estaba ocurriendo […] Esas personas se vieron directamente afectadas porque sus teléfonos celulares e internet no funcionaban".[337] Las comunicaciones permitieron, en un primer momento, la difusión de información crítica que llevo al diálogo libre en internet; la falta de éste llevó a las personas a la calle y, por ende, a la organización fuera de las computadoras.

Empero, una advertencia se desprende del análisis del proceso en Egipto, "[…] si va a tener éxito [el proceso de organización y protesta en internet], tiene que existir una masa crítica. Debe ocurrir rápido y necesita ganar, porque si no lo consigue la misma infraestructura que permite desarrollar un consenso rápido se utilizará para detectar y marginar a todos aquellos dedicados a sembrar el consenso".[338]

La vigilancia también se puede comprender como autocontrol. Si un individuo o una colectividad saben que la vigilancia existe, y que se puede aplicar tanto a particulares como a grupos, nace el fenómeno de la autocensura. Los criptopunks ponen a la vista que, además de la censura o autocensura, existen esquemas de interacción social en los que los individuos revelan su información de manera voluntaria. "Eso es Facebook, un modelo de negocio orientado a que la gente se sienta cómoda y revele su información"[339], la gente comparte a esta empresa su información de manera voluntaria y gratuita. "Y es importante relacionarlo únicamente con el aspecto humano, ya que no se trata de tecnología sino de controlar a través de la vigilancia. En cierto sentido, es el perfecto panóptico[340]", [341].

Además de lo señalado, los criptopunks resaltan el problema de la tecnología patentada, la cual pone candados para que el funcionamiento de la máquina sea incomprensible al usuario y sólo se destine a fines concretos, "pero en la actualidad el problema es mucho peor porque todos estos dispositivos están conectados con la red".[342] "Esta es la razón por la que el software

[337] Julian Assange, María Maestro (trad.), *Cypherpunks. La libertad y el futuro de internet*, *op.cit*., p.43.
[338] *Ídem.*
[339] Andy Müller-Maguhn en, Julian Assange, María Maestro (trad.), *Cypherpunks. La libertad y el futuro de internet*, *op.cit*., p. 45.
[340] Panóptico, definición en el glosario.
[341] Jacob Appelbaum, en Julian Assange, María Maestro (trad.), *Cypherpunks. La libertad y el futuro de internet*, *op.cit*., p.45.
[342] Julian Assange, María Maestro (trad.), Cypherpunks. La libertad y el futuro de internet, op.cit., p.51.

libre es tan importante para una sociedad libre".[343] El problema aquí planteado es de trascendental importancia, porque cercenan la libertad para comprender los procesos tecnológicos, y, por lo tanto, controlan o dirigen el avance del pensamiento humano. La revolución tecnológica de las comunicaciones atraviesa todas las esferas de la vida humana. Se ha sistematizado y computarizado el comportamiento de la humanidad.

Hay otra causa de vital importancia por la que los criptopunks buscan la creación de tecnología libre: la guerra en su fase tecnológica actual, la ciberguerra. "[La ciberguerra] […] se debe a que una serie de personas, quienes parecen ser 'los señores de la guerra', empiezan a hablar sobre tecnología como si la entendieran. […] y ninguno de ellos —ni siquiera uno— habla acerca de la ciberconstrucción de la paz, o de algo relacionado con la construcción de la paz. Hablan siempre de la guerra porque es su negocio, e intentan controlar los procesos tecnológicos y legales como medios para promover sus propios intereses. De modo que cuando no tenemos control sobre nuestra tecnología […] tratan de utilizarla para sus propios fines; concretamente para la guerra. Esta es la receta de cosas tan escalofriantes como el Stuxnet, […]"[344].

b) La militarización del ciberespacio

> Ahora existe una militarización del ciberespacio en el sentido de ocupación militar. Cuando te comunicas a través de internet, cuando te comunicas a través del teléfono celular –que ahora está enlazado a la red–, tus comunicaciones están siendo interceptadas por organizaciones de Inteligencia militar. […] Todos estamos bajo una ley marcial en lo que respecta a nuestras comunicaciones; simplemente no podemos ver los tanques, pero están. […] Es una militarización de la vida civil.[345]

¿Cómo se logra la militarización del ciberespacio? En el segundo capítulo se habló sobre la militarización del ciberespacio y su integración a la estrategia ofensiva y defensiva del Departamento de Estado. Aunado a la integración oficial, existen otros mecanismos para lograr

[343] Andy Müller-Maguhn en, Julian Assange, María Maestro (trad.), *Cypherpunks. La libertad y el futuro de internet*, *op.cit*., p. 51.
[344] Jacob Appelbaum, en Julian Assange, María Maestro (trad.), *Cypherpunks. La libertad y el futuro de internet*, *op.cit*., p.53.
[345]Julian Assange, María Maestro (trad.), *Cypherpunks. La libertad y el futuro de internet*, op.cit., p.55.

estos fines. El Laboratorio de Investigación de Seguridad y Privacidad de la Universidad de Washington invitó a Jacob Appelbaum a entrenar a un grupo de estudiantes de dicho centro académico, para participar en el concurso *Pacific Rim Collegiate Cyber Defense*.

Lo que sucede en este espacio son "ejercicios" para "[…] competir en una batalla cibernética donde SPAWAR (Space and Naval Warfare Systems Command/Comando de Sistemas de Guerra Espacial y Naval), un brazo civil de la marina estadunidense que realiza pruebas de penetración basadas en maniobras ofensivas y defensivas de piratería informática, desempeñaba el rol de *Red Team* (equipo rojo)."[346] Una prueba a la defensa cibernética de Estados Unidos, ¿qué tanto es un ejercicio académico? "Bueno, en su caso se limitan a patrocinar el juego porque quieren empezar a formar a los ciberguerreros del mañana". […] Había un agente de la CIA, […] el cuál ofrecía trabajo a los participantes […] Y la gente de SPAWAR estaba allí y también Microsoft".[347] El argumento, por supuesto, era defender a la nación y la Seguridad Nacional. "[…] te encontrabas frente a gente con bagaje bélico, […] tenían tanta guerra en el camino que por todos los medios trataban de enardecer el fervor patriótico de los participantes. […] lo evidente es que el gobierno de Estados Unidos está tratando de conseguir gente y está intentándolo por la vía del nacionalismo"[348].

Además, existe el almacenamiento masivo, "que no es otra cosa que almacenar todas las telecomunicaciones, todas las llamadas de voz, todo el tráfico de datos, cualquier modo en que los grupos consumen el Short Message Service (SMS o servicio de mensajes cortos), así como las conexiones a internet limitadas, en ocasiones, al correo electrónico".[349]

Por si todo esto fuera poco, los servicios militares armamentísticos tradicionales cuestan mucho más caros. Por poner un ejemplo: "puedes conseguir un buen almacenamiento de voz de todas las llamadas telefónicas efectuadas en Alemania anualmente por cerca de 30 millones de euros, gastos administrativos incluidos. Y el almacenamiento sólo cuesta alrededor de 8 millones de euros"[350], mientras que un avión militar cuesta "unos cien millones de dólares".[351]

---

[346] Jacob Appelbaum, en Julian Assange, María Maestro (trad.), *Cypherpunks. La libertad y el futuro de internet, op.cit.,* p. 56.
[347] *Ídem.*
[348] *Ibíd.,* pp.58 y 59.
[349] Andy Müller-Maguhn en, Julian Assange, María Maestro (trad.), *Cypherpunks. La libertad y el futuro de internet*, op.cit., p. 61.
[350] *Ibíd.,* pp. 61 y 62.
[351] Julian Assange, María Maestro (trad.), *Cypherpunks. La libertad y el futuro de internet*, op.cit., p.61.

c) Combatir la vigilancia total con las leyes del hombre

> Así que como ahora es un hecho que la tecnología posibilita la vigilancia total de las comunicaciones. […] en dónde trazar la línea para la supervisión judicial, y de qué modo delinear claramente el control que los ciudadanos puedan ejercer sobre el uso de dichas tecnologías.[352]

La discusión que plantean los criptopunks en esta sección, es el entredicho en que se colocan las supuestas democracias occidentales en lo que respecta a la vigilancia ilegal de los ciudadanos y al espionaje masivo. Como se planteó en el apartado anterior, invertir en vigilancia supone un costo mucho menor que la movilización de los actores estatales tradicionales del orden, entiéndase la policía y el ejército y sus respectivos servicios de Inteligencia.

3.3 Arquitectura de la opresión

3.3.1 Filtradores, *whistle-blowers*

El término *whistle-blower,* en su traducción literaria al español, quiere decir el que sopla un silbato o una alarma. Sin embargo, en el diccionario Oxford se define como "aquella persona que informa sobre otra persona u organización que se considera que participa en una actividad ilegal u inmoral"[353]. Acorde con el diccionario de Cambridge, es "aquella persona que le dice a alguna autoridad sobre algo ilegal que está sucediendo, particularmente en algún departamento gubernamental o compañía"[354]. Ambos términos cuentan con un valor positivo. Por ejemplo, una persona con acceso a cierta información se da cuenta que las acciones tomadas por personas o grupos dentro del ámbito al que pertenece no se realizan acorde con la ley o con base en principios éticos.

Los casos que a continuación se tratan son de personas que pertenecieron, con excepción de Julian Assange y Duncan Campbell, a los servicios de Inteligencia estadunidenses, y todos

[352] *Ibíd.,* p.69.
[353] *English Oxford Living Dictionaries*, en línea, entrada: "whistle-blower". [traducción propia]
[354] *Cambridge Dictionary*, en línea, entrada: "whistle-blower".

son de nacionalidades que pertenecen a la esfera de los *Five-Eyes,* comunidad de espionaje internacional de habla inglesa. Las revelaciones de todos llevaron, cada uno en su tiempo, a nuevas maneras de entender a las agencias de espionaje y su intrínseca relación con los gobiernos. Las revelaciones hechas por ellos cimbraron la pregunta: ¿espionaje para qué?, y la discusión, Seguridad *vs*. Libertad.

Las revelaciones hechas por Daniel Ellsberg y Duncan Cammpbell dejan ver que las actuales filtraciones en esta época tecnológica cuentan con antecedentes claros que responden a las mismas preocupaciones morales ya planteadas en el siglo pasado. Y también cómo los servicios de Inteligencia occidentales exponen los mismos motivos de antes para desarrollar acciones gubernamentales encubiertas y ajenas al escrutinio público. El enemigo ha cambiado, antes era la amenaza del comunismo, ahora es la amenaza del terrorismo, pero la justificación es la misma: garantizar la Seguridad Nacional.

3.3.1.1 Los Papeles del Pentágono

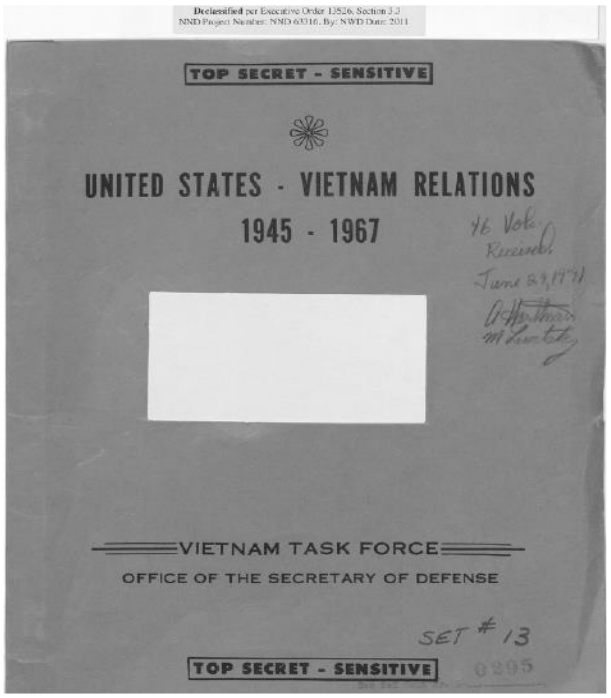
No se pretende hacer una explicación extensiva del caso los Papeles del Pentágono (*Pentagon Papers)* porque, por su importancia, son motivo de un estudio específico. Sin embargo, se hace un breve recuento del ambiente en el que se desarrolló la filtración, su impacto y la similitud entre ésta y los documentos Snowden.

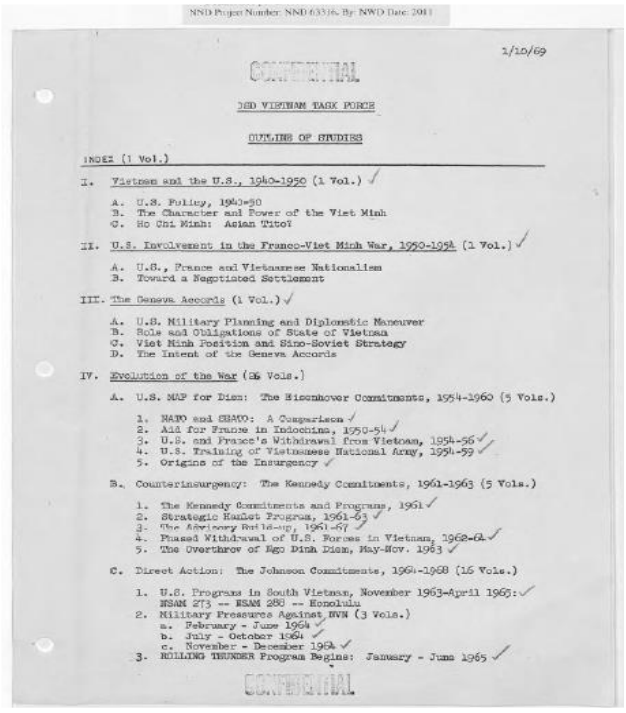
A inicios de los años setenta del siglo XX, con las tropas del ejército estadunidense en Vietnam, conmocionó a Estados Unidos y al mundo la revelación de documentos del Pentágono clasificados como *Top Secret-Sensitive.* Los documentos forman parte de un estudio histórico del involucramiento de Estados Unidos en Vietnam de 1945 a 1967. Y lo mandó elaborar quien fungió como secretario de la Defensa en las administraciones de John F. Kennedy y Lyndon B. Jonson: Robert S. McNamara. Los papeles fueron fotocopiados por el entonces analista militar y doctor en economía, Daniel Ellsberg, quien trabajaba en el *think tank* Rand Corporation. Se los brindó al periodista de *The New York Times,* Neil Sheeham.

El 13 de junio de 1971, la primera plana del referido periódico se intituló así: “Los archivos de Vietnam: estudio del Pentágono rastrea tres décadas del creciente involucramiento

de Estados Unidos"[355]. En la propia voz de Neil Sheehan, "el estudio del Pentágono va más allá de juicios históricos, sugiere que el interés estadunidense predominante fue primero la contención del comunismo y, después, la defensa del poder, influencia y prestigio de Estados Unidos. En ambas etapas no se tomaron en cuenta las condiciones de Vietnam".[356]

El estudio del Pentágono cuyo nombre oficial es Reporte de la Oficina del secretario de Defensa, los grupos operativos en Vietnam *(Report of the Office of the Secretary of Defense Vietnam Task Force),* en la actualidad se encuentra desclasificado y se puede consultar en la página de internet de los archivos del gobierno; "en el cuarenta aniversario de la filtración a la prensa; los Archivos Nacionales, junto con las bibliotecas presidenciales Kennedy, Johnson y Nixon han liberado el reporte completo. Hay cuarenta y ocho cajas y un aproximado de siete mil páginas desclasificadas. Treinta y cuatro por ciento del reporte está disponible por primera vez"[357]. Si las primeras filtraciones se hicieron en 1971, la desclasificación total se hizo en 2001, treinta años después, durante la presidencia de George W. Bush.





Fuente:www.archives.gov/research/pentagon-papers

[355] En inglés: *"Vietnam Archive: Pentagon Study Traces 3 Decades of Growing U. S Involvement"*
[356] Neil Sheehan, "Vietnam Archive: Pentagon Study Traces 3 Decades of Growing U. S Involvement", New York Achives/ 1971, The New York Times, 13 de junio de 1971, https://www.nytimes.com/1971/06/13/archives/vietnam-archive-pentagon-study-traces-3-decades-of-growing-u-s.html [traducción propia]
[357] "Pentagon Papers", s/a, en https://www.archives.gov/research/pentagon-papers [traducción propia] Los Papeles del Pentágo se encuentran completos en la liga.

Dos años después de las filtraciones, en 1973, en un primer juicio, "[Daniel] Ellsberg fue sentenciado a 105 años en prisión por robo y espionaje, siendo liberado después [de que la Suprema Corte declaró] la nulidad del juicio"[358]. El profesor e historiador estadunidense Douglas O. Linder creó el sitio web de internet *Famous Trials*, mismo que alberga la Universidad de Misuri. En él se encuentran los testimonios del juicio de Ellsberg en el que resalta lo siguiente: "las leyes de espionaje federal claramente apuntan a aquellos que brindaron a gobiernos extranjeros información clasificada, no a aquellos que dieron documentos al Congreso o a la prensa".[359] El juicio continuó, "el primer juicio a Ellsberg y Russo tuvo un súbito alto en julio de 1972 cuando se divulgó que el gobierno intervino una conversación entre uno de los acusados y su abogado o consejeros […] En noviembre la Suprema Corte votó con siete votos en contra y dos a favor, se negó a escuchar los argumentos de la defensa respecto de la escucha ilegal de las conversaciones por parte del gobierno. No obstante, […] el juez Byrne declaró juicio nulo y ordenó una nueva selección de jurado." [360]

En el segundo juicio, D. Ellsberg argumentó: "[…] 'sabía que ni una sola página (de los Papeles del Pentágono) podría dañar la defensa nacional si se le revelaban a alguien. Si hubiera creído lo contrario no lo habría copiado'. Ellsberg dijo que entregó los papeles con la esperanza de que las revelaciones que éstos contenían 'le pudieran dar al Congreso la confianza para terminar la guerra'".[361]

El segundo juicio también fue declarado nulo con base en un informe. Así, "el 27 de abril de 1973, el juez Byrne le entregó a la defensa un impactante memorándum, mismo que el fiscal del caso Watergate, Earl Silbert, brindó al fiscal general Henry Petersen. El memorándum decía que Silbert se enteró que 'Gordon Liddy y Howard Hunt asaltaron las oficinas del psiquiatra de Daniel Ellsberg para obtener los documentos siquiátricos de Ellsberg. […] Cuando se aclaró que el asalto se cometió por empleados de la Casa Blanca, siguiendo órdenes del presidente, las bases para un juicio nulo fueron convincentes".[362] Este hecho formó parte del caso Watergate.

Lo que demostraron los papeles del Pentágono fue, en primer lugar, la vinculación de la

[358] Dan Kedmey, "What's next for Snowden: 10 notorious leakers and how they fared", Time, 10 de junio de 2013, http://world.time.com/2013/06/10/10-notorious-leakers-and-how-they-fared/slide/daniel-ellsberg/ [traducción propia]
[359] Douglas O. Linder, "The Pentagon Papers (Daniel Ellsberg) Trial: An Account", Famous Trials, s/f, www.famous-trials.com/ellsberg/273-home [traducción propia]
[360] *Ídem.*
[361] *Ídem.*
[362] *Ídem.*

política exterior estadunidense con los procesos de autodeterminación de pueblos que no estuvieran alineados al "mundo libre", o a su programa económico.

En palabras de Noam Chomsky: "aunque es totalmente cierto que los gastos que le cuesta el imperio a una sociedad imperial pueden ser considerables, éstos quedan distribuidos sobre toda la población, en tanto que los beneficios revierten en sectores espaciales de la economía que, generalmente, se hallan bien representados en la elaboración de la política estatal. En la medida en que esto es cierto, un imperio resulta ser una forma de consolidación interna de poder y riqueza. Al mismo tiempo, proporciona mercados, fuentes de materias primas, mano de obra barata y oportunidades para realizar inversiones. Sobre la base de las afirmaciones de la teoría dominó, las ganancias a este respecto en Vietnam fueron considerables".[363] Con base en la teoría dominó, si caía Vietnam, caía el resto del sudeste asiático en el comunismo.

Al brindar a la opinión pública estos documentos, lo que quedó demostrado fue la falta de relación entre los hechos concretos y las decisiones tomadas por la Casa Blanca y el Pentágono.

Desde los años setenta se perseguía a quien filtrara información de interés público, se utilizaba la escucha ilegal de conversaciones, que fue en evolución conforme el desarrollo de la tecnología; se excluía al público de asuntos trascendentales en política exterior; y se confirmó la existencia del aparato de espionaje como institución lateral o alterna, que no pasa por otros poderes más que por el Ejecutivo y las agencias de Inteligencia. Es clave precisar que a partir de los Papeles del Pentágono y Watergate surge FISA.

Watergate demostró que el espionaje se utilizaba no sólo contra los países "enemigos" de Estados Unidos, sino también contra quien se opusiera al régimen, "donaban" millones de dólares de forma ilícita la compañía de comunicación más importante, las petroleras, y las aerolíneas; y se utilizaba la información para amedrentar a las voces disidentes.

> Varios testimonios sacaron a la luz los siguientes datos: 1. La Gulf Oil Corporation, la ITT (Compañía Internacional de Telégrafos y Teléfonos) y la American Airlines, además de otras grandes corporaciones americanas, habían hecho contribuciones ilegales -de millones de dólares- a la campaña Nixon. 2. En septiembre de 1971, poco después de

[363] Noam Chomsky, Hans Morgenthau, Manuela Díez (trad.), *El interés nacional y los documentos del Pentágono*, Barcelona, a. redondo, editor, 1973, p. 21.

> que *The New York Times* publicara las copias de los informes clasificados suministradas por Daniel Ellsberg -los *Pentagon Papers*- la administración planeó y llevó a cabo, con la participación personal de Howard Hunt y Gordon Liddy, un robo en la oficina del psiquiatra de Ellsberg, en busca de su historial. […] 4. Se descubrió que había desaparecido cierto material de los archivos del FBI. Se trataba de material asociado con una serie de escuchas telefónicas ilegales ordenadas por Henry Kissinger y llevadas a cabo en las líneas de cuatro periodistas y trece altos cargos del gobierno. Este material se encontraba en la Casa Blanca, en la caja fuerte del consejero de Nixon John Erlichman. 5. Uno de los ladrones de Watergate -Bernard Backer- contó al comité del Senado que también había estado implicado en un plan para atacar físicamente a Daniel Ellsberg, cuando éste estuviera hablando en una reunión pacifista en Washington. 6. Un testigo contó al comité del Senado que el presidente Nixon tenía grabaciones de todas las conversaciones privadas y todas las llamadas telefónicas de la Casa Blanca. Nixon se negó, en un principio, a entregar las cintas, y cuando por fin accedió a entregarlas éstas habían sido amañadas: habían sido borrados 18 minutos y medio de cinta. […] 9. Se reveló que durante más de un año (en 1969/1970) Estados Unidos había realizado bombardeos secretos y masivos en Camboya, hecho que se había ocultado al público estadunidense, incluido al Congreso.[364]

Daniel Ellsberg, a partir de la revelación de los documentos, se ha dedicado a luchar contra la secrecía de las agencias de Inteligencia. Ha sido un defensor incansable de Chelsea Manning, Julian Assange y Edward Snowden. "Si el día de hoy yo revelara los Papeles del Pentágono, la misma retórica y adjetivos se utilizarían contra mí. Me llamarían no sólo traidor, que me llamaron –lo que era falso y una calumnia-, me llamarían terrorista-, Bradley Manning y Julian Assange no son más terroristas que yo".[365]

También es uno de los fundadores de *Freedom of the Press Foundation,* "[…] la organización no gubernamental líder en la defensa de las libertades civiles en el mundo digital.

[364]Howard Zinn, Toni Strubel (trad.), "Capítulo 20, Los años setenta: ¿Bajo control?", *La otra historia de los Estados Unidos (desde 1492 hasta hoy)*, México, D.F., Siglo XXI, pp. 403 y 404.
[365] s/a, "Pentagon whistleblower Daniel Ellsberg: Julian Assange is not a terrorist", Democracy Now, 10 de diciembre de 2010, https://www.youtube.com/watch?v=5CHdzxgy9rw

Fundada en 1990, los defensores de EFF [las siglas de la organización] luchan por el derecho de los usuarios a la privacidad, libertad de expresión e innovación a través del impacto en las legislaciones, análisis de políticas públicas, activismo comunitario y desarrollo tecnológico. Trabajamos para asegurarnos que los derechos y libertades se mejoren y protejan a la par que crece el uso de la tecnología".[366] Ellsberg forma parte de la junta directiva de la organización, "en febrero de 2014, [Snowden] se unió a la junta directiva de la organización, y en 2016 fue nombrado su presidente".[367]

3.3.1.2 El caso GCHQ, Echelon y Duncan Campbell

En el primer capítulo se mencionó que Duncan Campbell y Mark Rosenball publicaron, en 1976, el artículo "Los fisgones" (*The eavesdroppers)*, mismo que daba cuenta del acuerdo firmado entre Estados Unidos y Gran Bretaña para la cooperación entre agencias de señales de inteligencia, SIGINT.

El acuerdo UKUSA y la red Echelon "constituyen un prototipo del sistema de escucha planetaria. [… que] procedió durante toda la guerra fría a interceptar y analizar las comunicaciones transmitidas a larga distancia, así como las señales de los cables submarinos y de los satélites comerciales. […] Después de la caída del muro de Berlín, esta red global reforzada por Internet se orientará hacia el espionaje industrial, en un entorno ultracompetitivo. Después del 11 de septiembre de 2001, este espionaje se situará en el centro de las estrategias securitarias."[368]

A pesar de las investigaciones de este periodista británico, los *Five-Eyes* se mantuvieron en relativa secrecía durante décadas, "[…] el lugar singular que la NSA ocupa en el entrecruzamiento de lo civil y lo militar, de lo político y lo económico en actividades tan clandestinas que las otras naciones de la coalición del mundo denominado libre no han sido informadas jamás del proyecto Echelon. No es sino hasta el fin del siglo XX que el Parlamento Europeo descubrirá su existencia". [369] Sin embargo, esto no fue motivo para que a través de los

[366] s/a, "About EFF", www.eff.org/es/about [traducción propia]
[367] S/a, "Board of directors", freedom.press/about/board/ [traducción propia]
[368] Armand Mattelart, Vitalis André, Juan Carlos Miguel de Bustos (trad.), *De Orwell al cibercontrol*, Barcelona, Gedisa, 2015, p. 95.
[369] *Ídem.*

años Duncan Campbell persistiera en el seguimiento puntual de las agencias de señales de Inteligencia.

El sitio en internet bajo el nombre *Duncan Campbell.org Investigative journalist & forensic expert,* alberga todos los artículos publicados que el investigador ha hecho del tema. Desde el primero, en mayo de 1976, hasta el último, en mayo de 1999. A continuación se presenta una síntesis de la información más importante para entender esta red a lo largo de la investigación de Duncan Campbell y de sus artículos.

Publicado en la revista *New Statesman* en febrero de 1979*,* con el título "La amenaza de los espías electrónicos" (*Threat of the electronic spies),* el artículo se centra en la GCHQ, la agencia británica homóloga de la NSA, y deja ver una de las interrogantes que aplica para ambas: "la GCHQ nunca ha atraído el mismo nivel de interés público que otras agencias de Inteligencia […]. De hecho, es más grande y potencialmente más siniestra, su influencia más extensa y las implicaciones de su trabajo amenazan más las libertades civiles y la paz mundial que todas las otras agencias juntas"[370]. El artículo también menciona la secrecía y el adoctrinamiento de los integrantes de esta agencia, se retrata al tratado UKUSA en general y el hecho de que "el pacto es jerárquico: en lo más alto se encuentra la Agencia de Seguridad Nacional (NSA), […] GCHQ tiene la posición de socio principal; Canadá, Australia y Nueva Zelanda son partes secundarias y las terceras partes incluyen a los aliados de la OTAN, de manera notable a Alemania y Noruega. Francia y Suecia son participantes y han mantenido vínculos con Finlandia, Sudáfrica y Brasil, entre otros."[371]

Además de la distribución territorial del planeta y de la coordinación entre las diversas agencias de recolección de señales para la uniformar los datos, léase red Echelon; la información recolectada se envía a la NSA. Otro punto de vital importancia en el artículo es el tipo de comunicaciones interceptadas: monitoreo de radio, satélites y comunicaciones, así como detección de cables submarinos, mediante los cuales hoy se transporta el cable de fibra óptica.

Sin embargo, no todo consiste en espiar las comunicaciones desde las bases tecnológicas, porque la participación de la NSA, desde entonces, ya podía apreciarse en el campo cinético; "[…] misiones provocadoras en espacio extranjero y marítimo son elemento habitual. […] El

[370] Duncan Campbell, "Threat of the electronic spies", New Statesman*,* 2 de febrero de 1979, p. 142 http://www.duncancampbell.org/menu/journalism/newstatesman/newstatesman-1979/Threat.pdf [traducción propia]
[371] *Ídem.*

incidente del Golfo de Tonkin, que Estados Unidos utilizó para justificar su entrada a la guerra de Vietnam, fue el resultado de una intrusión del *USS Maddox* [barco del cuerpo de marines], que ejercía trabajo de la NSA. Cuando el *USS Liberty* [barco de la armada] fue atacado por los israelíes […] en 1967, había tratado de monitorear las comunicaciones de Israel durante la Guerra de los seis días […] el incidente más reciente de este tipo fue la captura del *USS Pueblo* mientras espiaba en la costa de Corea del Norte."[372]

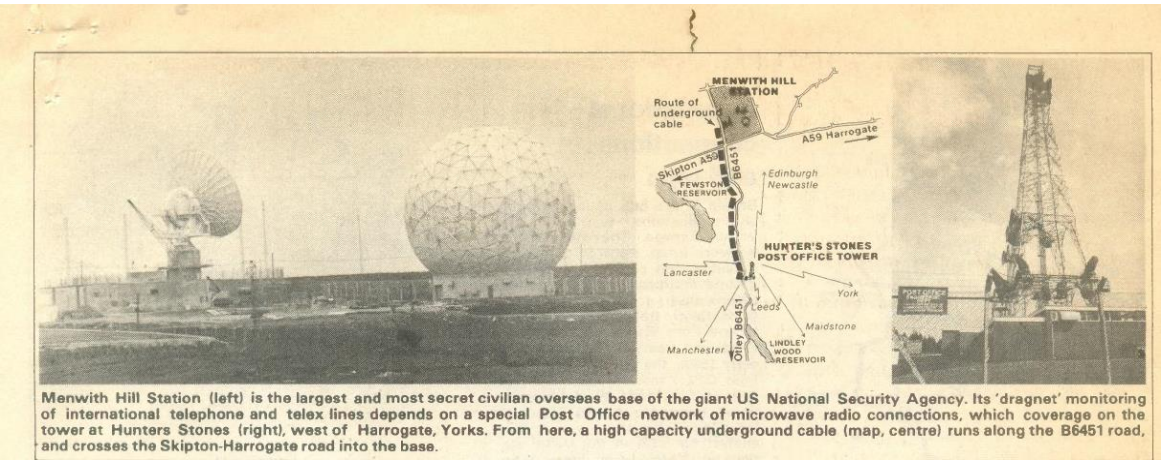
En este artículo, el autor recupera una trascendente cita del exdirector de la CIA, William Colby, expresada frente al Comité Church del Senado estadunidense. Aquel comité sacó a la luz pública los proyectos Shamrock y Minaret con los que espiaban a ciudadanos estadunidenses a través del teléfono y el telégrafo. "[…] el exdirector de la CIA, William Colby, admitió ante el Comité Church que la mayoría del éxito obtenido por la NSA se adquirió no por constantes y novedosos descubrimientos técnicos, sino por el robo de libros de código y 'contraseñas' de embajadas alrededor del mundo"[373].

En el artículo del 18 de julio de 1980, "La gran oreja de Estados Unidos en Europa" (*America´s big ear in Europe*), publicado también en la revista *New Statesman*; Duncan Campbell y Linda Melvern documentaron las actividades de una de las bases de la NSA en Gran Bretaña, cuyas instalaciones se encuentran en Menwith Hill. Describen cómo durante quince años "han analizado las comunicaciones de ciudadanos, corporaciones y gobiernos para obtener información de valor económico y político para la comunidad de Inteligencia de Estados Unidos. Desde los años sesenta, su más cercano socio en esta operación de creciente importancia en sofisticación técnica ha sido el servicio de correos británico".[374] El artículo continúa: "el servicio de correos británico ha construido Menwith Hill en el corazón del Sistema Nacional de Comunicaciones, y Gran Bretaña ocupa una posición nodal en las comunicaciones mundiales, en especial en Europa Occidental."[375]

Al recuperar una declaración del excoronel de la Fuerza Aérea de Estados Unidos, Fletcher Prousty, quien supervisó actividades de la NSA, se reproduce: "[…] en octubre de

[372] *Ibíd.,* pp. 142 y 143.
[373] *Ibíd.,* p. 145.
[374] Duncan Campbell y Linda Mervin, "America´s big ear in Europe", *New Statesman,* 18 de julio de 1980, p. 10. [traducción propia]
http://www.duncancampbell.org/PDF/America's%20Big%20Ear%20on%20Europe%2018%20July%201980.pdf
[375] *Ídem.*

1979, Pousty declaró: 'hay tres satélites sobre el Atlántico, cada uno es capaz de transmitir cerca de 20, 000 circuitos. Existen ocho cables trasatlánticos con cerca de 5, 000 circuitos. La NSA monitorea todos estos circuitos y graba la información electrónica transmitida, sus computadoras pueden recoger los mensajes que quieras al utilizar palabras clave'".[376] Este artículo evidenció la existencia de la *US Army Security Agency*, el brazo militar encargado del monitoreo en la NSA.



Fuente: *New Statesman.*[377]

En otro artículo de julio de 1980, intitulado "Thatcher, pinchada por sus aliados más cercanos" (*Thatcher Bugged by her 'closest ally*), escrito únicamente por Campbell, se declara lo mismo que décadas más tarde reconfirmaría Edward Snowden. La NSA también espía a sus aliados. "El gobierno británico es uno de los objetivos de las operaciones de monitoreo de las comunicaciones de la NSA, a pesar de las excepcionales instalaciones que Gran Bretaña les ha brindado en Menwith Hill".[378] Esta información se dio a conocer en 1975 a causa del *Fink Report to the House Committee on Government Operations and Individual Rights,* en el que "un estudio sobre la NSA reportó que: la NSA monitorea el tráfico de países específicos entre los que se incluye Gran Bretaña, nuestro aliado más cercano. El monitoreo del tráfico gubernamental se confirmó por un exempleado de la estación de Vint Hill Farms. Ésta tenía

[376] *Ídem.*
[377] Duncan Campbell y Linda Mervin, "America´s big ear in Europe", *New Statesman,* 18 de julio de 1980, p. 12. http://www.duncancampbell.org/PDF/America's%20Big%20Ear%20on%20Europe%2018%20July%201980.pdf [traducción propia]
[378] Duncan Campbell, "Thatcher Bugged by her 'closest ally", BBC Newsright, 25 de julio de 1980, p. 4. http://www.duncancampbell.org/menu/journalism/newstatesman/newstatesman-1980/Thatcher%20Bugged%20by%20her%20Closest%20Ally.pdf [traducción propia]

todo un banco de máquinas y equipo de personas, cuyo único trabajo era leer y procesar las comunicaciones británicas interceptadas".[379]

"Paradójicamente, el reporte secreto Fink que contiene estas referencias fue publicado sin atribución y pasando desapercibido en las audiencias de 1978 en la nueva *Foreign Intelligence Surveillance Act* [que resultó en la creación de la corte secreta de la FISA]"[380]. Esto en el marco del proyecto *Wideband Extraction* que comenzó a operar en 1969, ya con la extracción de datos de banda ancha. En el reporte se puntualiza la aparición de otras bases de escucha en Europa, por ejemplo: en Ausburgo, Alemania en el que trabaja el grupo 502d de la Agencia Armada de Seguridad; "Ausburgo se ha convertido en el 66º cuartel general del grupo de Inteligencia y seguridad";[381] además de tener dos sedes en Italia: Treviso y Brindisi y la de Sidi Yaha, cerca de Rabat en Marruecos, "esta base se dedica a interceptar las señales y cables franceses."[382]

El nombre de Duncan Campbell volvió a surgir en 1999. Fue el encargado de realizar un informe sobre la red Echelon para el Parlamento Europeo. "[…] el periodista escocés autor de la investigación que […] había revelado el nombre de código 'Echelon' y la amplitud del programa queda a cargo del trabajo. En la primavera de 1999 entrega su informe *Capacidad de interceptación 2000,* […] Campbell confirma: 'Este informe describe cómo, desde hace más de ochenta años, la información de Inteligencia electrónica adopta medidas para vigilar las comunicaciones internacionales (…) Existen sistemas inteligentes que interceptan y luego procesan todas las formas modernas de comunicación'. Para él esto es posible porque 'los países asociados a la NSA actualmente comparten cerca de ciento veinte sistemas de recolección de datos por satélite'".[383]

Las investigaciones del Parlamento Europeo sobre la Red Echelon se suspendieron a causa del 11 de septiembre de 2001. No se hablaría nuevamente de ésta hasta junio de 2013 con motivo de las filtraciones de Edward Snowden.

[379] *Ídem.*
[380] *Ídem.*
[381] *Ídem.*
[382] *Ídem.*
[383] Antoine Lefébure, Bárbara Poey Sowerby (trad.), *El caso Snowden. Así espía Estados Unidos al mundo*, *op.cit.,* p. 102.

3.3.1.3 WikiLeaks y Julian Assange

Como ellos mismos se definen en su página de internet, "WikiLeaks es una entidad mediática multinacional y una biblioteca virtual. Fue fundada en 2006 por su editor Julian Assange."[384] A diferencia de otros medios, contiene la publicación de material específico cuya obtención no es común; "WikiLeaks se especializa en el análisis y publicación de grandes volúmenes de información oficial, censurada o restringida que involucra guerra, espionaje o corrupción."[385] Para su fundador, "WikiLeaks es una biblioteca de dimensiones monumentales que almacena los documentos más perseguidos del mundo. Nosotros les damos asilo, los analizamos, promovemos y obtenemos más."[386]

Los acontecimientos siguientes, presentados en orden cronológico, nos ayudarán a ubicarnos temporalmente para comprender el desenlace de la situación actual de WikiLeaks y el impacto que ha tenido en las relaciones internacionales. Comprenden el año, el nombre original de la publicación así como una breve descripción. Todos estos documentos y su publicación sucedieron antes de la liberación en internet del video "Asesinato Colateral (*Collateral Murder)*."

Fecha de publicación	Documento/ Nombre de la filtración	Descripción
12/ 2006	*Series/Inside Somalia and the Union of Islamic Courts*	"Documentos estratégicos de los dos bandos de la guerra en Somalia y la apuesta por el involucramiento de China."[387]
7/11/ 2007	*Camp Delta Standard Operating Procedure*	"Procedimientos operativos para los grupos de operación [*Join Tak Force Guantanamo (JTF-GTMO)]* en Campo Delta (la prisión de Guantánamo). Este es el documento principal de 238 páginas para la operatividad de Guantánamo, incluye los lineamientos de seguridad y el trato a los detenidos. El documento extenso contiene formas, tarjetas de identidad e incluso instrucciones de sepelios musulmanes. Está firmado por el Mayor General Millar, quien tiempo después fue enviado por Donald Rumsfeld a Abu Ghraib para *guantanamizarlo*. El documento también es motivo de una acción legal entre la

[384] s/a, "What is WikiLeaks", 3 de noviembre de 2015 en https://WikiLeaks.org/What-is-WikiLeaks.html [traducción propia]
[385] *Ídem.*
[386] *Ídem.*
[387] "Inside Somalia and the Union of Islamic Courts", WikiLeaks, diciembre de 2006, en https://WikiLeaks.org/wiki/Inside_Somalia_and_the_Union_of_Islamic_Courts [traducción propia]

		Unión Estadunidense por las Libertades Civiles (ACLU), quien ha tratado de obtenerlo, y el Departamento de Defensa, que lo retuvo por completo […] El documento expone […] los métodos sistemáticos para evitar que los prisioneros se reúnan con miembros de la Cruz Roja, así como el uso de extremo estrés psicológico como forma de tortura".[388]
Después de la publicación de los procedimientos operativos en Guantánamo, WikiLeaks fue clausurada, pero encontró servidores en Alemania y Bélgica para continuar con la divulgación del material.		
24/03/2008	*Church of Scientology collected Operating Thetan documents*	"[Este archivo contiene] la colección de 'Biblias' secretas de Cienciología, un culto global fundado por el autor de ciencia ficción, L. Ron Hubbard, y popularizado por celebridades de Hollywood […] La mayoría del material se verificó por el Centro de Tecnología Religiosa perteneciente a la Cienciología"[389]; dicho centro demandó a WikiLeaks por publicar material no permitido registrado bajo derechos de autor.
21/ 11/ 2009	*Climatic Research Unit emails, data, models, 1996-2009* [Watergate climático]	"Este archivo publica más de 60 megabytes de correos electrónicos, documentos, código y modelos de la Unidad de Investigación de cambio climático de la Universidad de East Anglia [Reino Unido], escritos entre 1996 y 2009".[390]

Así como la historia de los Papeles del Pentágono está ligada a la de Daniel Ellsberg, la historia de WikiLeaks y su fundador van de la mano. Incluso, según la Enciclopedia Británica, "para la creación de WikiLeaks, [Julian Assange] se inspiró en la publicación de los Papeles del Pentágono por Daniel Ellsberg".[391] Aunque ya en funciones, como se observa en el cuadro anterior, fue hasta abril de 2010 cuando la organización sobresalió a los ojos del mundo. El lunes 5 de abril de ese año apareció en la red de redes, internet, el video "Asesinato Colateral", cuya entrada comienza con el epígrafe: "El lenguaje político está diseñado para hacer que las mentiras parezcan verdades; el asesinato, respetable, y dar apariencia de solidez al viento", George Orwell.[392].

[388] "Camp Delta Standard Operating Procedure", WikiLeaks, 7 noviembre de 2007, en https://WikiLeaks.org/wiki/Camp_Delta_Standard_Operating_Procedure [traducción propia]
[389] "Church of Scientology collected Operating Thetan documents"; WikiLeaks, 8 de marzo de 2008, en https://WikiLeaks.org/wiki/Church_of_Scientology_collected_Operating_Thetan_documents
[390] "Climatic Research Unit emails, data, models, 1996-2009, WikiLeaks, 21 de noviembre de 2009, en https://WikiLeaks.org/wiki/Climatic_Research_Unit_emails,_data,_models,_1996-2009 [traducción propia]
[391] Entrada: WikiLeaks, Enciclopedia Británica, https://www.britannica.com/topic/WikiLeaks [traducción propia]
[392] *Collateral Murder,* WikiLeaks, Irak, en https://collateralmurder.WikiLeaks.org [traducción propia]

3.3.1.3.1 Daño colateral

El video más visto dura 17 minutos, aunque existe también la versión larga, de 39 minutos. En blanco y negro, la secuencia de imágenes muestra el asesinato de doce civiles en el suburbio de Nuevo Bagdad en Irak. Filmado desde un helicóptero Apache con armas de 30 mm., se encuentran miembros del ejército estadunidense que narran el desenlace desde las alturas mientras disparan las armas.

Los hechos: se cuentan doce muertes. Entre ellas, dos periodistas de Reuters Saeed Chmagh y Namir Noor-Eldeen; dos niños heridos y su padre asesinado víctimas de una segunda ráfaga de disparos al tratar de ayudar a las primeras víctimas. A pesar de las evidencias videográficas, "el ejército de Estados Unidos alegó que las víctimas murieron en una batalla entre fuerzas estadunidenses e insurgentes. "No hay duda que las fuerzas de coalición claramente estuvieron involucradas en operaciones de combate contra fuerzas hostiles". Lugarteniente Coronel Scott Bleichwehl, vocero de las fuerzas estadunidenses en Bagdad, *The New York Times.*"[393]

Después de estos acontecimientos, el grupo mediático Reuters pidió, a través de la *Freedom of Information Act,* el video para aclarar lo sucedido, pero nunca se le entregó. El ejército de Estados Unidos se mantuvo firme en la versión de que las víctimas quedaron entre dos fuegos y no violó las reglas internacionales de combate.

Fuente: Andrew Winning—Reuters/Landov[394]

[393] *Ídem.*
[394] Andrew Winning, *WikiLeaks founder Julian Assange at press conference, 2010,* Reuters/Landov,

3.3.1.3.2 Los diarios de guerra

Afganistán

Tres meses después de la publicación de "Asesinato Colateral", WikiLeaks publicó la primera parte de los documentos que después se conocerían como "Los diarios de guerra de Afganistán e Irak" (*War Logs)*. Actualmente estos documentos se pueden consultar en el sitio *wardiaries.WikiLeaks.org*. "Los documentos son el conjunto de aproximadamente 391, 000 reportes que cubren la guerra en Iraq de 2004 a 2009, y en Afganistán de 2004 a 2009".[395]

El 25 de julio de 2010 se publicaron "Los diarios de guerra de Afganistán" (*Afghanistan War Logs*). WikiLeaks argumentó, al respecto, que la verdad de la ocupación se revelaba en los documentos filtrados. "Una gran cantidad almacenada de archivos militares secretos de Estados Unidos el día de hoy provee un retrato devastador de la fallida guerra en Afganistán: revela cómo las fuerzas de coalición han matado cientos de civiles en incidentes sin reportar, los ataques talibanes se han elevado y los comandantes de la Organización del Tratado del Atlántico Norte (OTAN) temen que la vecindad con Pakistán e Irán alimenten la insurgencia".[396]

Los documentos también mostraban la actuación secreta de los grupos militares de las fuerzas aliadas, mismos que violaron de forma sistemática las reglas de combate internacionales. Los documentos filtrados de los registros en Afganistán muestran:

- "Una unidad secreta de fuerzas especiales [llamada *black]*, a la caza de líderes talibanes para ejecutarlos o capturarlos sin juicio alguno.
- "Estados Unidos encubrió evidencia de que los talibanes adquirieron sistemas anti misiles, SAM (*Surface-to-air missile, SAM*)
- "La coalición [Estados Unidos, Reino Unido, Canadá, Australia, Alianza del Norte] aumenta el uso de drones Reaper [General Atomics MQ-9 Reaper, también conocido como Predator B. Vehículo Aéreo no tripulado (UAV)] para cazar y matar objetivos talibanes a control remoto desde una base en Nevada.

---

https://www.britannica.com/topic/WikiLeaks

[395] s/a, "Iraq & Afghan War Diaries", War Diaries, WikiLeaks, en https://wardiaries.WikiLeaks.org [traducción propia]

[396] Nick Davies, David Leigh, "Afghanistan war logs: Massive leak of secret files exposes truth of occupation", The Guardian, 25 julio de 2010, en https://www.theguardian.com/world/2010/jul/25/afghanistan-war-logs-military-leaks

- "Los talibanes han causado una creciente carnicería con una masiva escalada de bombas en los caminos que ha matado a más de 2, 000 civiles."[397]

Irak

Los diarios de guerra de *Irak (The Iraq War Logs)* fueron publicados meses después de los de Afganistán, el 22 de octubre de 2010. Según la propia WikiLeaks, "es la mayor filtración de documentos clasificados en la historia".[398]"La filtración se constituye con 391, 832 documentos de la guerra y la ocupación en Irak, del primero de enero de 2004 al 31 de diciembre de 2009 […] [Cada documento pertenece a los reportes llamados] Acción Significativa en la Guerra, [*Significant Action in the war, SIGACT].*" [399]

Según el periódico inglés *The Guardian*, los documentos detallan:

- "Las autoridades estadunidenses no investigaron cientos de reportes de abusos, tortura, violación e incluso asesinato de la policía iraquí y soldados cuya conducta es aparentemente sistemática y no recibe castigo alguno.
- "Un helicóptero de combate estadunidense […] mató a insurgentes después de que se rindieron.
- "Más de quince mil civiles murieron en incidentes desconocidos. Estados Unidos y Reino Unido han insistido en que no existen registros oficiales de bajas civiles pero, en los registros de las bitácoras, existen 66, 081 muertes de no combatientes de un total de 109, 000 muertos.
- "Los numerosos reportes de abuso a los detenidos, con evidencia basada en sustento médico, describen a los prisioneros encadenados, vendados de los ojos, colgados de muñecas y tobillos, así como víctimas de azotes, golpes, patadas y electroshocks. Seis reportes reportan la aparente muerte del detenido."[400]

Al respecto, en México *La Jornada* documentó la conferencia de prensa que ofreció Julian

[397] *Ídem.*
[398] s/a, War Diaries, WikiLeaks, https://WikiLeaks.org/irq/ [traducción propia]
[399] *Ídem.*
[400] Nick Davies, Jonathan Steele y David Leigh, "Iraq war logs: secret files show how US ignored torture", The Guardian, 22 de octubre de 2010, https://www.theguardian.com/world/2010/oct/22/iraq-war-logs-military-leaks [traducción propia]

Assange en representación de WikiLeaks, junto con la asociación civil *Iraq Body Count*, días después de la publicación de los documentos en defensa de su postura de divulgación. En Londres, J. Assange dijo que "el Pentágono, de forma extraordinaria, pidió (a WikiLeaks) […] que ese material fuera destruido […] quería destruir totalmente esta información a fin de privar de ella a la población, a fin de que las víctimas sean privadas de justicia. Esa amenaza de atacar […] (a WikiLeaks) en virtud de la Ley de espionaje ha sido proferida contra la prensa del mundo entero. Nosotros no toleraremos ese tipo de violación de la libertad de prensa."[401]

Por su parte, el argumento del Pentágono para condenar la filtración fue el siguiente: "Crea una laguna que puede hacer que asesinen a nuestras tropas y a aquellos que pelean. Nuestros enemigos aprovecharán esta información para buscar información de cómo operamos, (nosotros) conservamos nuestras fuentes y reaccionamos en situaciones de combate, incluso (sobre) las capacidades de nuestro equipamiento."[402]

La asociación civil *Iraq Body Count,* la cual llevó el registro de las muertes no contabilizadas por las fuerzas de ocupación, "calculó que los archivos muestran unas 15 mil muertes de civiles desconocidas hasta el momento"[403].

3.3.1.3.3 Biblioteca pública de la diplomacia estadunidense

El 28 de noviembre de 2010, meses después de las filtraciones de Los diarios de guerra, WikiLeaks sorprendió con una nueva filtración, en este caso sobre las comunicaciones entre el gobierno estadunidense y sus embajadas en el mundo, denominado *Cablegate.* La filtración se encuentra dividida en cinco secciones: 1) Los cables diplomáticos de Kissinger 1973-1976; 2) Los cables diplomáticos de Carter, 1977; 3) los cables diplomáticos de Carter 2, 1978; 4) Los cables diplomáticos de Carter 3, 1979 y 5) *Cablegate*, casi todos los cables diplomáticos de 2003 a 2010. También se pueden consultar según las siguientes clasificaciones: *unclassified, confidetial, limited official use, secret, unclassified // for oficial use only, confidential // noforn*

[401] s/a, con información de AFP, DPA, Reuters, PL y The Independent, "Con los archivos se muestra ´la verdad el baño de sangre en Irak´: *WikiLeaks",* La Jornada, Mundo, domingo 24 de octubre de 2010, p. 24.
[402] Nick Davies, Jonathan Steele y David Leigh, "Iraq war logs: secret files show how US ignored torture", The Guardian, 22 de octubre de 2010, https://www.theguardian.com/world/2010/oct/22/iraq-war-logs-military-leaks [traducción propia]
[403] [403] s/a, con información de AFP, DPA, Reuters, PL y The Independent, "Con los archivos se muestra ´la verdad el baño de sangre en Irak´: *WikiLeaks",* La Jornada, Mundo, domingo 24 de octubre de 2010, p. 24.

y *secret//noforn.* [404]

Sin embargo esta filtración, a pesar de su cercanía en el tiempo con las dos anteriores, difirió de éstas en un factor que demostraría ser fundamental. WikiLeaks publicó en su página de internet los primeros cables diplomáticos al mismo tiempo que lo hicieron cinco periódicos, *The Guardian* en Reino Unido, *The New York Times* en Estados Unidos, *Der Spiegel* en Alemania, *El País* en España y *Le Monde* en Francia. En la siguiente cita se muestra el tono de lo que sería la respuesta estadunidense:

> La administración Obama ordenó a los empleados federales que mantuvieran como clasificado el material filtrado por WikiLeaks, pese a que esta información estaba siendo publicada por algunas de las agencias de noticias más importantes del mundo, incluidos los diarios *The New York Times* y *The Guardian.* Los empleados recibieron la consigna de que el acceso al material, ya fuera a través de WikiLeaks.org o de *The New York Times*, se consideraba violación a la seguridad. Tanto las agencias gubernamentales como la Biblioteca del Congreso, el Departamento de Comercio y el Ejército de Estados Unidos bloquearon el acceso al material de WikiLeaks a través de sus respectivas redes. La prohibición no se limitaba únicamente al sector público. Los empleados del gobierno de Estados Unidos advirtieron a las instituciones académicas que los estudiantes que quisieran hacer carrera en el sector público debían evitar todo contacto con las informaciones reveladas por WikiLeaks en sus investigaciones y en su actividad en la red.[405]

Entre las revelaciones más importantes del *Cablegate* sobresalen las siguientes:

- "Afirmaciones de que Rusia y sus agencias de Inteligencia usan jefes de la mafia para llevar a cabo operaciones criminales, […] la relación es tan cercana que el país se ha vuelto 'un virtual país mafioso'.
- "Críticas devastadoras de comandantes estadunidenses, del presidente y oficiales locales de Afganistán sobre la participación de Gran Bretaña en Sangin […]

[404] s/a, "Plus D. Public Library of US Diplomacy", WikiLeaks, https://WikiLeaks.org/plusd/
[405] Julian Assange, María Maestro (trad.*), Cypherpunks. La libertad y el futuro de internet*, *op. cit.,* p.33.

- "Los cables contienen imputaciones específicas de corrupción, así como severas críticas de las embajadas estadunidenses a sus países anfitriones desde las islas caribeñas hasta China y Rusia. El material incluye referencias a Putin como –perro alfa--, a Hamid Karzai como –paranoico–, mientras Angela Merkel supuestamente evita tomar riesgos y no es creativa, así como comparaciones entre Mahmoud Ahmadinejad y Adolfo Hitler.
- "Los cables […] revelan el uso de las embajadas de Estados Unidos como parte de una red global de espionaje, en la que se les encarga a sus diplomáticos no sólo obtener información de las personas con las que se reúnen, sino detalles personales, como números frecuentes de viajes aéreos, detalles de tarjetas de crédito e incluso material de ADN.
- "Clasificado como directivos de inteligencia humana expedido por Clinton y su predecesora Condoleezza Rice, instruyeron a oficiales para reunir información de instalaciones militares, marcajes de armas, detalles de los vehículos de líderes políticos así como escáneres del iris, huellas dactilares y ADN.
- "El objetivo más controvertido fue el de las autoridades de Naciones Unidas. Esa directiva *[Human Intelligence Directives]* solicitó las especificaciones de las telecomunicaciones y de los sistemas de tecnologías de la información usados por los oficiales de mayor rango y su equipo, detalles de redes VIP usados para comunicaciones oficiales con la intención de incluir datos actualizados, medidas de seguridad, contraseñas y llaves de encriptación personales".[406]

3.3.1.3.4 La respuesta de Estados Unidos frente a la filtración de los cables diplomáticos

El vocero del Departamento de Estado en ese entonces, PJ Crowley, declaró: "Les aseguro que nuestros diplomáticos son sólo eso, diplomáticos. No se involucran en actividades de Inteligencia. Representan a nuestro país alrededor del mundo, mantienen contacto abierto y transparente con otros gobiernos, así como con figuras públicas y privadas y eso es lo que

[406] David Leigh, "US embasy cable leak sparks global diplomatc crisis", The US embasy cables, The Guardian, Sun 28 Nov 2010, https://www.theguardian.com/world/2010/nov/28/us-embassy-cable-leak-diplomacy-crisis

reportan. Eso es lo que los diplomáticos han hecho por cientos de años".[407]

Por su parte, *The New York Times* tituló a ocho columnas "Los cables filtrados ofrecen una cruda mirada de la diplomacia estadunidense (*Leaked Cables Offer Raw Look at U.S Diplomacy)".*[408] Días antes de la publicación de los documentos, hubo un intercambio epistolar entre el gobierno de Estados Unidos y Julian Assange. Ahora son públicas cinco cartas.

Fecha	De	Para	Contenido
26-10- 2010	Julian Assange, Editor en jefe de WikiLeaks	Embajador Louis B. Susman	[En] "respuesta a declaraciones públicas del gobierno de Estados Unidos sobre preocupaciones de la posible publicación de WikiLeaks (WL) y otros medios, derivado de supuestas grabaciones del gobierno. "[…] WikiLeaks tiene como objetivo, la permanente divulgación de la mayor cantidad de información en interés del público, WL estará agradecida si el gobierno de Estados Unidos le nombra de forma privada cualquier caso específico (números de informes o nombres), donde considere que la publicación de información puede poner en riesgo a personas […] WikiLeaks respetará la confidencialidad de los consejos del gobierno de EEUU y está preparado para cumplir estas solicitudes sin tardanza alguna.
27-10-2010	Harold Hongju Koh, asesor jurídico del Departamento de Estado	Jennifer Robinson, abogada de Julian Assange y al Sr. Assange	"Escribo en respuesta a la carta del 26 de noviembre que dirigió al embajador de EEUU Lous B. Susman respecto de su intención de publicar nuevamente en su sitio WikiLeaks lo que usted dice que son documentos clasificados del gobierno. "Como usted sabe, si alguno de los materiales que intenta publicar se los proveyó cualquier oficial del gobierno, o cualquier intermediario sin autorización; se los dieron en violación de la ley de Estados Unidos sin miramientos a las graves consecuencias de esta acción. Mientras WikiLeaks tenga dicho material, la violación a la ley persiste. "Entendemos por conversaciones con representantes del *The New York Times, The Guardian* y *Der Speigel*, que WL también les ha dado 250, 000 documentos a cada uno para publicar, esto fomenta la diseminación ilegal de documentos clasificados. "La publicación de documentos de esta naturaleza como mínimo: • Pondrá en riesgo la vida de incontables

[407] *Ídem.*

[408] Scott Shane y Andrew W. Lehren, "Leaked Cables Offer Raw Look at U.S Diplomacy", Mundo, The New York Times, 28 de noviembre de 2010, https://www.nytimes.com/2010/11/29/world/29cables.html

			inocentes […] • Pondrá en riesgo operaciones militares en marcha […] [contra] actores que amenazan la seguridad global, y • Pondrá en riesgo la cooperación entre países, socios, aliados y actores comunes que confrontan […] terrorismo, enfermedades pandémicas, proliferación nuclear y amenazan la estabilidad global. […] si genuinamente está interesado en parar el daño de sus acciones, debe: 1) asegurarse que WL termine la publicación de cualquier material, 2) asegurarse que WL regrese todos los materiales […], 3) remover y destruir todos los registros de sus bases de datos.
28-10-2010	Julian Assange, Editor en jefe de WikiLeaks	Embajador Louis B. Susman	"[…] WikiLeaks no tiene deseo de poner a personas en riesgo o daño, ni deseamos dañar la Seguridad Nacional de Estados Unidos. "WL empleó tiempo y recursos significantes, en redactar el material en nuestra posesión para lograr esto y verificar nuestro trabajo y el de nuestros pares de los medios tradicionales. "Le escribí explícitamente para ofrecerle al gobierno de EEUU la posibilidad de nombrar casos específicos [para borrar de los documentos]. En vez de eliminar el riesgo que ustedes alegan sufrirán las personas y operaciones militares, rechazaron nuestra oferta de un diálogo constructivo y se decidieron por un enfoque de confrontación. La respuesta nocturna del Departamento de Estado no es más que un comunicado de prensa jurídico, que se confirma con el hecho de que ustedes se lo dieron a la prensa. […] "Entiendo que el gobierno preferiría que la información que se publicará no fuera de dominio público y que no esté a favor de la transparencia. Esto dicho, hay un riesgo o no lo hay. Han escogido responder de una manera que me lleva a concluir que los supuestos riesgos son por completo extravagantes y, por el contrario, están preocupados en suprimir evidencia de abusos a los derechos humanos y otros comportamientos criminales. Procederemos a divulgar el material bajo los estándares de nosotros y nuestros socios en la prensa, al menos que me contacten como prometieron en la llamada con nuestros abogados el viernes pasado.
Fin del intercambio epistolar			

28-10-2010	Declaración de la oficina de prensa del Departamento de Estado	Para publicación inmediata	"Nos anticipamos a la divulgación de lo que suponen serán cientos de miles de cables clasificados del Departamento de Estado. Por su naturaleza, la información que se reporta a Washington [los cables] es sin malicia e incompleta. No expresa nuestra política, ni determina nuestras decisiones de política exterior. […] dicha publicación pone en riesgo a nuestros diplomáticos, profesionales de la Inteligencia y a personas alrededor del mundo que vienen a EEUU para solicitar ayuda en promover la democracia y la transparencia gubernamental. […] El presidente Obama apoya la transparencia responsable en casa y alrededor del mundo, pero esta acción riesgosa e irresponsable va en contrasentido de esa meta. […] WikiLeaks ha puesto en riesgo no sólo la causa por los derechos humanos, también las vidas y el trabajo de esos individuos. Condenamos, en los más fuertes términos, la publicación no autorizada de documentos clasificados e información sensible para la Seguridad Nacional. [409]

Fuente: Tabla de elaboración y traducción propia con información de las cartas publicadas en *The New York Times.*

3.3.1.3.5 No maten al mensajero

El 19 de junio de 2012 Julian Assange entró a la embajada de Ecuador, en Londres. El motivo, solicitar asilo político. En el presente año, 2018, se cumplieron seis años sin que pueda salir de la misma; los últimos seis meses se le ha cortado toda comunicación. En ese entonces, 2012, Assange entró como ciudadano australiano y solicitó asilo conforme a lo establecido en la Convención sobre el Estatuto de los Refugiados de 1951, bajo el argumento de ser perseguido político y en riesgo de ser extraditado a un tercer país. Los cuatro países involucrados: Ecuador, Estados Unidos, Suecia y Reino Unido forman parte de la convención antes mencionada.

El entonces ministro de Relaciones Exteriores y Movilidad Humana de Ecuador, Ricardo Armando Patiño Aroca, en rueda de prensa convocada el 16 de agosto de 2012, para abordar tanto las amenazas por parte del Reino Unido a su sede diplomática en Londres y la solicitud de Julian Assange de asilo diplomático; declaró, en nombre del gobierno ecuatoriano, la decisión de brindar asilo político al fundador de WikiLeaks.

[409] s/a, "Letters between WikiLeaks and the U.S Government", The New York Times, s/f, https://www.nytimes.com/interactive/projects/documents/letters-between-WikiLeaks-and-gov#document/p5

En la resolución del grupo de trabajo sobre detenciones arbitrarias de la ONU, UNWGAD, por sus siglas en inglés, que se manifestó sobre el caso de Julian Assange, afirmó que sí es una detención arbitraria al contravenir los artículos 9 y 10 de la Declaración Universal de Derechos Humanos; y los artículos 7, 9(1), 9(3), 9(4), 10 y 14 del Pacto Internacional de Derechos Civiles y Políticos. Dichos artículos establecen que:

> *Declaración Universal de Derechos Humanos; proclamada y aprobada en 1948 por la Asamblea General de las Naciones Unidas.*
>
> Artículo 9
>
> Nadie podrá ser arbitrariamente detenido, ni preso ni desterrado.[410]
>
> Artículo 10
>
> Toda persona tiene derecho, en condiciones de plena igualdad, a ser oída públicamente y con justicia por un tribunal independiente e imparcial, para la determinación de sus derechos y obligaciones o para el examen de cualquier acusación contra ella en materia penal.[411]
>
> *Pacto Internacional de Derechos Civiles y Políticos, el cual entró en vigor el 23 de marzo de 1976.*
>
> Artículo 7
>
> Nadie será sometido a torturas ni a penas o tratos crueles, inhumanos o degradantes. En particular, nadie será sometido sin su libre consentimiento a experimentos médicos o científicos.[412]
>
> Artículo 9
>
> (1)Todo individuo tiene derecho a la libertad y a seguridad personal. Nadie podrá ser sometido a detención o prisión arbitrarias. Nadie podrá ser privado de su libertad, salvo

[410] s/a, *Declaración Universal de Derechos Humanos*, Yacine Ait Kaci (ilustraciones), Naciones Unidas, 2015, p.20.
[411] *Ibíd,* p.22.
[412] s/a, *Pacto Internacional de Derechos Civiles y Políticos,* Naciones Unidas, Derechos Humanos, Oficina del Alto Comisionado, Adoptado y abierto a la firma, ratificación y adhesión por la Asamblea General en su resolución 2200 A (XXI), de 16 de diciembre de 1966, en https://www.ohchr.org/sp/professionalinterest/pages/ccpr.aspx

por las causas fijadas por ley y con arreglo al procedimiento establecido en ésta.

(3) Toda persona detenida o presa a causa de una infracción penal será llevada sin demora ante un juez u otro funcionario autorizado por la ley para ejercer funciones judiciales, y tendrá derecho a ser juzgada dentro de un plazo razonable o a ser puesta en libertad. La prisión preventiva de las personas que hayan de ser juzgadas no debe ser la regla general, pero su libertad podrá estar subordinada a garantías que aseguren la comparecencia del acusado en el acto del juicio, o en cualquier momento de las diligencias procesales y, en su caso, para la ejecución del fallo.

(4) Toda persona que sea privada de libertad en virtud de detención o prisión tendrá derecho a recurrir ante un tribunal, a fin de que éste decida, a la brevedad posible, sobre la legalidad de su prisión y ordene su libertad si la prisión fuera ilegal.[413]

Artículo 10

(1) Toda persona privada de libertad será tratada humanamente y con el respeto debido a la dignidad inherente al ser humano.

(2) a) Los procesados estarán separados de los condenados, salvo en circunstancias excepcionales, y serán sometidos a un tratamiento distinto, adecuado a su condición de personas no condenadas; b) Los menores procesados estarán separados de los adultos y deberán ser llevados ante los tribunales de justicia con la mayor celeridad posible para su enjuiciamiento.[414]

Artículo 14

(1) Todas las personas son iguales ante los tribunales y cortes de justicia. Toda persona tendrá derecho a ser oída públicamente y con las debidas garantías por un tribunal competente, independiente e imparcial, establecido por la ley, en la substanciación de cualquier acusación de carácter penal formulada contra ella o para la determinación de sus derechos u obligaciones de carácter civil. La prensa y el público podrán ser excluidos de la totalidad o parte de los juicios por consideraciones de moral, orden público o Seguridad Nacional en una sociedad democrática, o cuando lo exija el interés de la vida privada de las partes o, en la medida estrictamente necesaria en opinión del

[413] *Ídem.*
[414] *Ídem.*

tribunal, cuando por circunstancias especiales del asunto la publicidad pudiera perjudicar a los intereses de la justicia; pero toda sentencia en materia penal o contenciosa será pública, excepto en los casos en que el interés de menores de edad exija lo contrario, o en las acusaciones referentes a pleitos matrimoniales o a la tutela de menores.

(1) Toda persona acusada de un delito tiene derecho a que se presuma su inocencia mientras no se pruebe su culpabilidad conforme a la ley.

(3) Durante el proceso, toda persona acusada de un delito tendrá derecho, en plena igualdad, a las siguientes garantías mínimas:

a) A ser informada sin demora, en un idioma que comprenda y en forma detallada, de la naturaleza y causas de la acusación formulada contra ella;

b) A disponer del tiempo y de los medios adecuados para la preparación de su defensa y a comunicarse con un defensor de su elección;

c) A ser juzgado sin dilaciones indebidas;

d) A hallarse presente en el proceso y a defenderse personalmente o ser asistida por un defensor de su elección; a ser informada, si no tuviera defensor, del derecho que le asiste a tenerlo, y, siempre que el interés de la justicia lo exija, a que se le nombre defensor de oficio, gratuitamente, si careciere de medios suficientes para pagarlo;

e) A interrogar o hacer interrogar a los testigos de cargo y a obtener la comparecencia de los testigos de descargo y que éstos sean interrogados en las mismas condiciones que los testigos de cargo;

f) A ser asistida gratuitamente por un intérprete, si no comprende o no habla el idioma empleado en el tribunal;

g) A no ser obligada a declarar contra sí misma ni a confesarse culpable.

(4) En el procedimiento aplicable a los menores de edad a efectos penales se tendrá en cuenta esta circunstancia y la importancia de estimular su readaptación social.

(5) Toda persona declarada culpable de un delito tendrá derecho a que el fallo condenatorio y la pena que se le haya impuesto sean sometidos a un tribunal superior, conforme a lo prescrito por la ley.

(6) Cuando una sentencia condenatoria firme haya sido ulteriormente revocada, o el

condenado haya sido indultado por haberse producido o descubierto un hecho plenamente probatorio de la comisión de un error judicial, la persona que haya sufrido una pena como resultado de tal sentencia deberá ser indemnizada conforme a la ley, a menos que se demuestre que le es imputable en todo o en parte al no haberse revelado oportunamente el hecho desconocido.

(7) Nadie podrá ser juzgado ni sancionado por un delito por el cual haya sido ya condenado o absuelto por una sentencia firme de acuerdo con la ley y el procedimiento penal de cada país.[415]

3.3.1.4 El caso Snowden

Fue George Bush el que autorizó los programas de espionaje electrónico que serían de dominio público después del compendio de información filtrado por Edward Snowden. Por lo que hemos visto, los programas de espionaje electrónico surgen desde mediados del siglo XX. No es la primera vez que sucede algo así, basta recordar los Papeles del Pentágono y la renuncia del presidente Richard Nixon en los años setenta. Siendo así, ¿en qué radica la importancia de las filtraciones de Snowden?

El 6 de junio de 2013, el periódico *The Guardian* publicó en primera plana, el primero de una serie de artículos acerca de los programas de espionaje estadunidense efectuados por la NSA, también conocidos como el programa del presidente. El mismo día se hizo pública la entrevista realizada por el periodista Glenn Greenwald a Edward Snowden, misma que fue filmada por la documentalista Laura Poitras y posteriormente distribuida como el documental llamado *Citizenfour*.

El documental se proyectó en 2014 y ganó múltiples reconocimientos internacionales, entre ellos los premios Óscar y BAFTA a mejor documental. *Citizenfour* pertenece a una trilogía que explica la política exterior y las políticas securitarias estadunidenses posteriores al 11 de septiembre de 2001.[416]

---

[415] *Ídem.*

[416] Anteriormente, Laura Poitras filmó *My country, My country* (2006), ésta es la primera película de la trilogía, cuyo argumento se centra en las primeras elecciones en Irak después de la invasión de Estados Unidos en 2003. La segunda parte de la trilogía *The Oath* (2010), relata la historia de un hombre que fue guardaespaldas de Osama Bin Laden y que ahora es taxista en Afganistán, por último cierra esta magistral exposición con *Citizenfour* (2014).

El último trabajo que se conoce de Poitras es *Risk* (2016), mismo que tardaría seis años en filmar y cuyo tema es WikiLeaks y su fundador. Su trabajo la llevó a "demandar al gobierno de Estados Unidos para saber por qué ha sido, en múltiples ocasiones, sujeta a acosos kafkianos en aeropuertos alrededor del mundo."[417] Entre los abusos de los que ha sido víctima menciona que "la han detenido en las fronteras más de cincuenta ocasiones entre 2006 y 2012, hasta por cuatro horas cada vez. En varias ocasiones, menciona, le han dicho distintos agentes que se encuentra en la lista para 'no volar' [*No Fly list]*, le han confiscado y retenido hasta por 41 días su equipo electrónico, y también la han amenazado con esposarla por tomar notas. El último incidente tuvo lugar mientras trabajaba en un filme sobre el fundador de WikiLeaks, Julian Assange."[418]

Con anterioridad, "Poitras dijo que en 2006, después de volver a Estados Unidos al término de la filmación de su documental *My Country, My Country*, la colocaron en la lista de vigilancia del Departamento de Seguridad del Interior […] le asignaron la más alta calificación de amenaza, aunque nunca ha sido acusada de un crimen. La detuvieron en múltiples ocasiones hasta 2012, cuando el periodista Glenn Greenwald escribió un artículo sobre sus experiencias."[419]

A estos periodistas es a los que Snowden decide compartirles los archivos copiados de la NSA. Snowden trabajó para Booz Allen Hamilton como analista de infraestructura de la NSA, voló a Hong Kong donde se reunió con ambos. Los documentos que les compartió revelarían, entre otras cosas, los dos programas de espionaje con mayor alcance en la historia de la humanidad.

La imagen que se encuentra enseguida corresponde a la portada del periódico *The Guardian* del jueves 6 de junio de 2013.

[417] Ben Child, "Citizenfour director Laura Poitras sues US over 'Kafkaesque harassment'", *The Guardian,* 14 de julio de 2015,https://www.theguardian.com/film/2015/jul/14/citizenfour-director-laura-poitras-sues-us-harassment-edward-snowden [traducción propia]
[418] *Ídem.*
[419] *Ídem.*


Thursday 06.06.13
Published in London and Manchester
£1.40

theguardian
guardian.co.uk

US orders phone firm to hand over data on millions of calls

Exclusive Top secret court ruling demands 'ongoing, daily' data from Verizon

Glenn Greenwald

The National Security Agency is currently collecting the telephone records of millions of US customers of Verizon, one of America's largest telecoms providers, under a top secret court order that was issued in April.

The order, a copy of which has been obtained by the Guardian, requires Verizon on an "ongoing, daily basis" to give the NSA information on all telephone calls in its systems, both within the US and between the US and other countries.

The document shows for the first time that under the Obama administration the communication records of millions of US citizens are being collected indiscriminately and in bulk – regardless of whether they are suspected of any wrongdoing.

The secret Foreign Intelligence Surveillance Court (Fisc) granted the order to the FBI on 25 April, giving the government unlimited authority to obtain the data for a specified three-month period ending on 19 July.

Under the terms of the blanket order, the numbers of both parties on a call are handed over, as is location data, call duration, unique identifiers, and the time and duration of all calls. The contents of the conversation itself are not covered.

The disclosure is likely to reignite long-standing debates in the US over the proper extent of the government's domestic spying powers. Under the Bush administration, officials in security agencies had disclosed to reporters the large-scale collection of call records data by the NSA, but this is the first time significant and top-secret documents have revealed the continuation of the practice on a massive scale under President Barack Obama.

The unlimited nature of the records being handed over to the NSA is extremely unusual. Fisc orders typically direct the production of records pertaining to a specific named target who is suspected of being an agent of a terrorist group or foreign state, or a finite set of individually named targets.

The Guardian approached the National Security Agency, the White House and the Department of Justice for comment in advance of publication last night. All declined. The agencies were also offered the opportunity to raise specific security concerns regarding the publication of the court order.

The court order expressly bars Verizon from disclosing to the public either the existence of the FBI's request for customers' records, or the court order itself. "We decline comment," said Ed McFadden, a Washington-based Verizon spokesman.

The order, signed by Judge Roger Vinson, compels Verizon to produce to the NSA electronic copies of "all call detail records or 'telephony metadata' created by Verizon for communications between the US and abroad" or "wholly within the US, including local telephone calls".

The order directs Verizon to "continue production on an ongoing daily basis thereafter for the duration of this order". It specifies the records to be produced include "session identifying information", such as "originating and terminating number", the duration of each call, telephone calling card numbers, trunk identifiers, International Mobile

Continued on page 4 »

Fuente: https://thesocietypages.org/cyborgology/files/2013/06/guardian-6june2013.jpg

El artículo intitulado "La NSA recolecta millones de registros telefónicos al día de clientes de Versión" *(NSA collecting phone records of millions of Verizon customers daily)*, dejó al descubierto uno de los programas de espionaje de la NSA, el que se refiere a la recolección en masa de la metadata de los registros telefónicos. Este programa fue aprobado bajo la sección 215 del Acta Patriota. La NSA solicitó el registro diario de las comunicaciones telefónicas de Verizon por adelantado, ya fueran entre ciudadanos en Estados Unidos, o ciudadanos en territorio estadunidense cuyas comunicaciones se establecieran entre ellos y personas en el extranjero.

Sin embargo en principio, y por las modificaciones a la ley basadas en las investigaciones del Comité Church, que llevaron a la creación de FISA, la NSA se dedica al espionaje en el extranjero. El documento filtrado en el que se basa el artículo escrito por Glenn Greenwald, "[…] muestra, por primera vez, que bajo la administración Obama se recolectan indiscriminadamente y en masa los millones de archivos de millones de ciudadanos estadunidenses, -sin importar si son o no sospechosos de actos malos".[420]

Veamos una breve cronología de hechos trascendentes:

- 6 de junio de 2013. Aparece en el periódico *The Guardian* la noticia intitulada "La NSA recolecta millones de registros telefónicos al día de clientes de Verizon". Se hace público el video "No quiero vivir en una sociedad que haga ese tipo de cosas: Edward Snowden, filtrador de la NSA'".
- 1 de agosto de 2013. Rusia concede asilo a Edward Snowden.

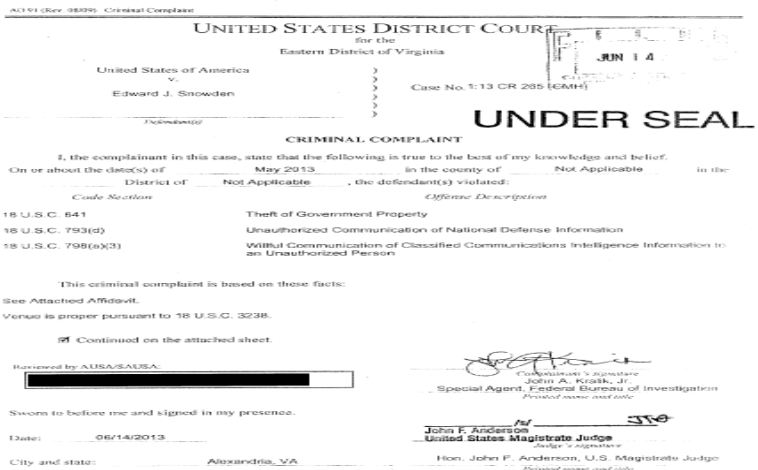
[420] Glenn Greenwald, "NSA collecting phone records of millions of Verizon customers daily", The Guardian, 6 de junio de 2013, https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order [traducción propia]

- 9 de agosto de 2013. Conferencia de prensa de Obama: La vigilancia de la NSA. Snowden y las relaciones Estados Unidos-Rusia.[421]

Hasta este punto, en agosto de 2013, el gobierno de Estados Unidos decide hacerlo público, aunque ya lo conocía. La denuncia penal que interpuso el gobierno contra Snowden data de mayo de 2013. En el caso "Estados Unidos de América vs. Edward J. Snowden" suscrito a la Corte del Distrito Este de Virginia, se le imputaron cargos por violaciones a tres secciones del código penal.

1. 18 U.S.C 641 Robo a propiedad gubernamental.
2. 18 U.S.C 793 (d) Comunicaciones no autorizadas de información de defensa nacional.
3. 18 U.S.C 798 (a) (3) Comunicar, de manera intencionada, información clasificada de Inteligencia de las comunicaciones a una persona no autorizada.

En el primer capítulo del subtema "Marco Jurídico de la Comunidad de Inteligencia, subtema Ley de espionaje" se describe que las secciones 793 y 798 pertenecen a la Ley de espionaje formulada en 1917. Edward Snowden está acusado de violar leyes promulgadas bajo el contexto de la Primera Guerra Mundial. A continuación se comparte la denuncia penal.



AO 91 (Rev. 08/09) Criminal Complaint

UNITED STATES DISTRICT COURT
for the
Eastern District of Virginia

JUN 14

United States of America
v.
Edward J. Snowden
Defendant(s)

Case No. 1:13 CR 265 (CMH)

UNDER SEAL

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.
On or about the date(s) of May 2013 in the county of Not Applicable in the
District of Not Applicable, the defendant(s) violated:

Code Section	Offense Description
18 U.S.C. 641	Theft of Government Property
18 U.S.C. 793(d)	Unauthorized Communication of National Defense Information
18 U.S.C. 798(a)(3)	Willful Communication of Classified Communications Intelligence Information to an Unauthorized Person

This criminal complaint is based on these facts:
See Attached Affidavit.
Venue is proper pursuant to 18 U.S.C. 3238.

☑ Continued on the attached sheet.

Reviewed by AUSA/SAUSA:
[redacted]

Complainant's signature
John A. Kralik, Jr.
Special Agent, Federal Bureau of Investigation
Printed name and title

Sworn to before me and signed in my presence.

Date: 06/14/2013

/s/
John F. Anderson
United States Magistrate Judge
Judge's signature

City and state: Alexandria, VA

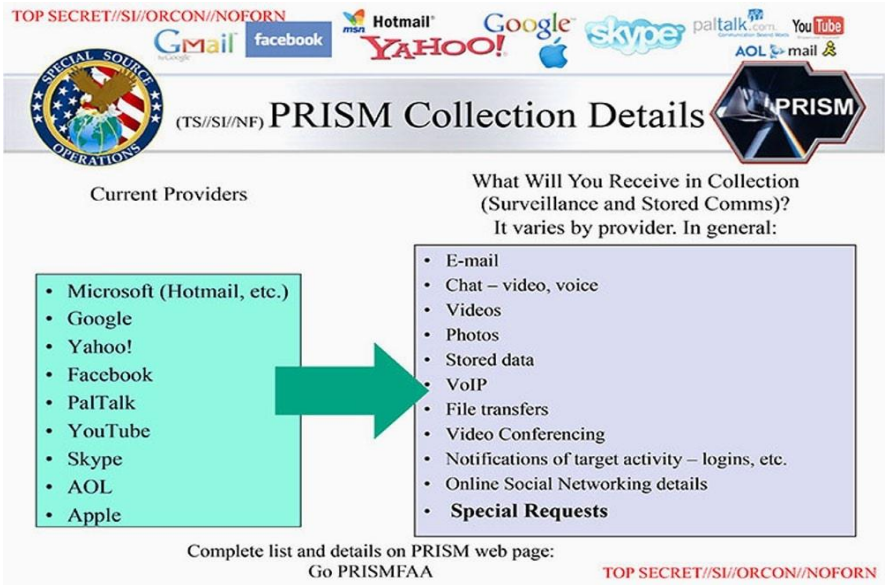
Hon. John F. Anderson, U.S. Magistrate Judge
Printed name and title

Fuente: *The Washington Post*[422]

[421] "Complete Obama Press Conference on NSA Surveillance, Snowden & US-Russia Relations- August 9, 2013", Youtube, https://www.youtube.com/watch?v=paZgOC7Wqo0

Las principales filtraciones se refieren a los programas PRISM y UPSTREAM. Aunque en el primer capítulo vimos cómo funcionan éstos programas, no se mencionaron ejemplos de su impacto real. En el artículo de *The Intercept,* "La redada. En operativo frustrado de espionaje, la NSA tuvo como objetivo a activista en favor de la democracia" (*The raid. In Bungled Spying Operation, NSA targeted Pro-Democracy Campaigner* [423], se relata la historia del activista naturalizado neozelandés Tony Fullman, primer objetivo de PRISM en ser reconocido públicamente. "Detalles de la vigilancia se encuentran en documentos brindados a *The Intercept* por el filtrador de la NSA, Edward Snowden. Más de 190 páginas de registros del más alto nivel de secrecía de comunicaciones interceptadas que datan de mayo a agosto de 2012 muestran que la agencia utilizó el polémico sistema de vigilancia de internet, PRISM, para interceptar los mensajes de Gmail y Facebook de Fullman y otros defensores de la democracia en Fiji. Fullman es la primera persona en el mundo en ser identificada y confirmada como un objetivo de PRISM."[424]

En la diapositiva de siguiente se describen las actividades de PRISM según la NSA.



Fuente: The Intercept[425]

---

[422] s/a, "U.S. vs. Edward J. Snowden criminal complaint", The Washington Post, https://apps.washingtonpost.com/g/documents/world/us-vs-edward-j-snowden-criminal-complaint/496/

[423] Ryan Gallagher y Nicky Hager, "The raid. In Bungled Spying Operation, NSA targeted Pro-Democracy Campaigner", The Intercept, 15 agosto de 2016, https://theintercept.com/2016/08/14/nsa-gcsb-prism-surveillance-fullman-fiji/

[424] *Ídem.*

[425] *Ídem.*

3.4 Freedom of Information Act, USC 5 SS 552

La Ley de libertad de la información, FOIA, por sus siglas en inglés, por una buena razón no se encuentra en la sección jurídica que aparece en el primer capítulo. En sentido inverso de las leyes que aparecen ahí, el marco jurídico del espionaje en Estados Unidos, la Ley de acceso a la información ha permitido conocer muchas de las prácticas de espionaje. Podríamos decir que esta ley es un contrasentido de las leyes ahí mencionadas.

3.4.1 Marco histórico de la ley de Libertad a la Información

El primer antecedente de la ley se sitúa en 1955, durante la presidencia de Dwight D. Eisenhower. En ese entonces fue propuesto un proyecto de ley por el congresista del partido Demócrata, John Moss, ante el aumento de la secrecía gubernamental en el marco de la Guerra Fría. Este primer intento no consiguió el apoyo que se necesitaba del Partido Republicano, por lo que no se legisló. Durante la presidencia de Lyndon B. Johnson, el presidente "[…] se opuso a la ley -de hecho, todas las agencias y departamentos de la administración federal se opusieron a ella-- […]"[426]. Aunque es en esta presidencia cuando por primera vez se aprueba la ley, se hace con una serie de modificaciones que la constreñían.

Fue hasta después de los escándalos de Watergate, en 1974, que "[…] el Congreso enmendó FOIA para que se convirtiera en la ley que es ahora. El Senado y la Casa [de representantes] introdujeron nuevos requisitos, marcos de tiempo, sanciones para la información denegada y un necesario lenguaje para exonerar a periodistas y grupos de interés públicos."[427]

3.4.2 Ley de la libertad a la información electrónica

La enmienda a la Ley de acceso a la información llamada, Ley de acceso a la información electrónica (*Electronic Freedom of Information Act),* fue la tercera sufrida por esta ley. Nos enfocaremos sólo en ella ya que las otras dos están relacionadas con temas de combate a las drogas.

El 2 de octubre de 1996, el entonces presidente William J. Clinton firmó la enmienda a la

[426] s/a, "History of FOIA", Electronic Frontier Foundation, https://www.eff.org/es/issues/transparency/history-of-foia [traducción propia]
[427] *Ídem.*

ley cuyo nombre completo es: *Electronic Freedom of Information Act of 1996.* En la declaración de la firma de la enmienda, el entonces presidente dijo: "FOIA fue la primera ley en establecer un derecho legal efectivo de acceso a la información gubernamental, enfatizando la necesidad crucial en una democracia del acceso abierto a la información por parte de los ciudadanos […]"[428].

El principal argumento para esta enmienda, de hace poco más de veinte años, fue la necesidad de transferir la información gubernamental a nuevos formatos tecnológicos, es decir del papel al *Cd-Rom*, disquetes y páginas web, los formatos electrónicos de entonces. Como argumentó el expresidente Clinton: "La legislación que firmo hoy trae a FOIA a la edad electrónica al clarificar que aplica a los archivos que se mantienen en formato electrónico. […] A medida que el gobierno disemina activamente mayor cantidad de información, espero que disminuya la necesidad de utilizar FOIA para obtener información gubernamental."[429] En esta enmienda se extendió el periodo para responder a peticiones hechas al gobierno a través de FOIA, de diez a veinte días. La intención fue que las agencias brindaran más información a los ciudadanos y, por consiguiente, mayor transparencia.

Después del 11 de septiembre de 2001, FOIA sufrió un revés. El presidente George W. Bush firmó el 5 de noviembre de 2001 la orden ejecutiva 13233. "La ley de libertad de información es una las herramientas legales más importantes que tienen los ciudadanos y periodistas para promover la transparencia del gobierno en Estados Unidos. Sin embargo, la historia muestra que empoderar a los ciudadanos ha preocupado a muchos miembros de la rama ejecutiva, incluyendo a presidentes de ambos partidos […]"[430].

[428] *Electronic Freedom of Information Act Amendments of 1996,* United States Department of Justice, https://www.justice.gov/oip/electronic-freedom-information-act-amendments-1996 [traducción propia]
[429] *Ídem.*
[430] s/a, "History of FOIA", Electronic Frontier Foundation, https://www.eff.org/es/issues/transparency/history-of-foia [traducción propia]

Conclusiones

Real Politik versus justicia internacional

> "Tienes que determinar qué es lo que importa para ti: vivir sin libertad pero cómodamente ¿es algo que estás dispuesto a aceptar? Y creo que muchos lo aceptamos, […] puedes despertarte todos los días, ir a trabajar, cobrar tu sueldo […] en contra del interés general, e ir a dormir después de ver tus programas de televisión. Pero, si te das cuenta que ese es el mundo que ayudaste a crear, y que se va a poner peor de generación en generación, que se extenderán las capacidades de este tipo de arquitectura de la opresión, te das cuenta de que estás dispuesto a aceptar cualquier riesgo, no importa cuál sea el resultado mientras el público pueda tomar sus propias decisiones de cómo todo esto se aplica".[431]
>
> E.Snowden

Tal vez el cuestionamiento más importante de este trabajo es acerca de la creencia de que las agencias de Inteligencia sirven a la democracia estadunidense para mantenerse e imponerse. No obstante, consideramos que la hipótesis principal, al concluir este trabajo, se reformula. El discurso de la democracia, la libertad y la seguridad, en cualquiera de sus versiones, ya sea en el marco de la Guerra Fría o con la actual multidimensionalidad de los conflictos, le sirve a la matriz tecnológica, militar e industrial para perpetuar el poder que obtuvo después de la Segunda Guerra Mundial y que, con el paso del tiempo, se ha fortalecido.

Podemos incluso revertir el orden de la argumentación del geopolítico Z. Brzezinski. Como se señaló en la cita del capítulo dos, para éste la democracia estadunidense y sus instituciones ejercen un atractivo que se refuerza con el dominio de las comunicaciones, el

[431] Laura Poitras, Glenn Greenwald, "NSA whistleblower Edward Snowden: 'I don´t want to live in a society that does these sort of things'", The NSA files, The Guardian, 9 de junio de 2013, https://www.theguardian.com/world/video/2013/jun/09/nsa-whistleblower-edward-snowden-interview-video

aparato militar y la tecnología de punta. Sin embargo, el dominio de la tecnología, utilizado en el ámbito militar para el espionaje y la cooptación de las empresas de las comunicaciones elaboran la ilusión de una democracia.

Por eso no sorprende que durante las administraciones de George W. Bush y de Barack H. Obama existieran mínimos cambios, o ninguno, en las dirigencias de las agencias que componen a la Comunidad de Inteligencia. Bush fue el presidente que autorizó los programas de vigilancia masiva que filtró Edward J. Snowden. Y Obama fue el presidente que lo persiguió. Julian Assange publicó los diarios de guerra de Afganistán e Irak durante ambas administraciones. Y la administración de Obama la que lo confinó a vivir en la embajada de Ecuador, en Londres. Chealsea Manning, la filtradora de los documentos a WikiLeaks, bajo la administración Obama fue condenada por traición. La Inteligencia, en consecuencia, no es un asunto de gobierno, sino de Estado.

En la introducción mencionamos que estudiar los aparatos de Inteligencia en su modalidad actual nos podría ayudar a comprender el proyecto de nación que se esconde detrás de la fachada libertaria de Estados Unidos. En cierto sentido estaba equivocada. Si analizamos sólo desde la perspectiva de la coyuntura, cometeremos muchos errores**.** Cuando inicie la presente investigación tenía la idea de que las revelaciones de los filtradores demostraban un abuso de poder del gobierno, pero que las acciones de éste respondían al cuadro internacional de la guerra contra el terrorismo; entonces, en cierto sentido estaban justificados, no los medios pero sí los fines, de tal forma que a lo que habría que oponerse es a la manera, no a la causa.

Pero al profundizar en el estudio, la información me remontó en el tiempo. Partí del último capítulo y luego marché hacia atrás, hasta topar con la promulgación de la Ley de Seguridad Nacional de 1947. Tal vez después de leer la tesis ya no resulte impactante la información develada por las filtraciones Snowden. Sin embargo, es imprescindible aclarar este punto. Como antes señalé, empecé de atrás hacia adelante. Por tanto, me encontré con información histórica de programas de espionaje posteriores a la Segunda Guerra Mundial gracias a la curiosidad por entender cómo funcionan los servicios de espionaje y del ejército que WikiLeaks y los archivos Snowden brindaron al público internacional.

Tanto la vigilancia masiva que mostraron las revelaciones de Edward Snowden como el arsenal de guerra cibernética con el que cuenta Estados Unidos no obedecen a un momento

coyuntural. No. El 11 de septiembre de 2001 fue el pretexto para comenzar, de forma legal, a hacer acopio de grandes cantidades informáticas de datos a través de la NSA y de sus socios comerciales. El aparato técnico-militar-industrial, que con la tecnología actual resulta de dimensiones panópticas, se inscribe en lo civil. Empero, por lo que hemos podido observar, si no hubiera sido el 11 de septiembre de 2011, otro suceso hubiera servido para poner en marcha estos programas. ¿Por qué me atrevo a afirmar esto? Porque existen programas anteriores. En efecto, PRISM y UPSTREAM no surgen de la nada, tienen detrás de ellos una estructura tecnológica y de investigación. ¿Para qué? Aquí me permito hacer una propuesta: "[…] la información se convierte en el elemento fundamental de la hegemonía mediante las tecnologías de recolección de información e Inteligencia. Es la ciberguerra**…**"[432]

Seguridad Nacional

La tecnocracia militar-industrial se sustenta en componentes ideológicos de alto alcance. El concepto de Seguridad Nacional es recurrente tanto para justificar la vigilancia como para condenar a los disidentes de la misma. Todo se hace en nombre de ella, concepto que, por lo demás, abarca todo lo que el Estado quiera abarcar. Recordemos que en el diccionario de términos de la defensa se entiende la Seguridad Nacional como todos los intereses de Estados Unidos más su política exterior. Es un concepto que supera los alcances soberanos, no está circunscrito a ningún territorio, está relacionado con la construcción constante de un enemigo, no con un ataque específico, y se aplica a cualquier dominio, incluso a aquella abstracción denominada espacio cibernético.

La Seguridad Nacional es la justificación permanente de la guerra preventiva. Es un asunto de geoestrategia. Viéndolo a través de los lentes de la Historia, no podíamos esperar que Estados Unidos actuara de manera distinta, pues como potencia imperial intentará dominar cada nuevo lugar de disputa que se le presente. Hoy es el espacio cibernético, durante la Guerra Fría fue el espacio sideral; hace cien años, "la era anterior, la de la hegemonía de la flota, había sido testigo de la multiplicación, desde finales del siglo XIX, de las bases navales

[432] Armand Mattelart, *Historia de la sociedad de la información.,* p. 167.

estadunidenses en territorio extranjero, verdaderos enclaves que escapan a la soberanía del país anfitrión."[433]

Prism y Upstream muestran la capacidad de la NSA para recolectar información a través de las telecomunicaciones, las armas cibernéticas para imponer un proyecto en el ciberespacio; todo en el marco de la globalización y de la ideología de mercado. Google, Facebook, Microsoft, Yahoo, Amazon introducen el componente económico en la ecuación. Todas estas compañías figuran entre las más ricas a nivel mundial y cuentan con el beneficio de su ámbito de influencia que es todo el mundo conectado a la red. No es sorpresa, en consecuencia, que Facebook cuente con centros de datos en distintos puntos del orbe, ni que Google sea el motor de búsqueda más utilizado. Así como antes los intelectuales de las más costosas universidades de Estados Unidos oscilaban entre la academia y el gobierno; ahora son los gerentes de *Silicon Valley* los que oscilan entre el soleado y *cool* San Francisco y el centro del poder político que es Washington. Y que además cotizan en Wall Street.

Nos encontramos en un mundo de neologismos: "sociedad de la información", "redes sociales", "neutralidad de la red", "tuitear", "acceso a la información", y aunque no todos éstos pueden ponerse en la misma canasta, es evidente que son términos que surgen con la tecnología de las democracias occidentales. Cualquier país que no permite el acceso de sus ciudadanos a Facebook, viola la libertad de información y, por tanto, su sociedad está oprimida. En sentido contrario, recordemos que el lingüista Noam Chomsky subraya la injerencia de este gigante de las redes sociales en las elecciones en Alemania, o toda la información que brindaron las compañías al gobierno estadunidense a petición de órdenes judiciales sin avisarle a sus usuarios.

Armand Mattelart, al cuestionar el concepto de sociedad de la información nos dice que "la sociedad global de la información se ha convertido en un reto geopolítico, y el discurso que la envuelve es una doctrina sobre las nuevas formas de hegemonía. […] la hegemonía mundial pasa por las tecnologías tecnotrónicas[434] y se manifiesta a través de una triple revolución: diplomática, militar y gerencial."[435]

---

[433] Armand Mattelart, *Gilles Multigner (trad.), Un mundo vigilado,* Barcelona, Paidós, 2009, .p. 71.
[434] Tecnotrónico, ver glosario.
[435] Armand Mattelart, *Gilles Multigner (trad.), Un mundo vigilado,* Barcelona, Paidós, 2009, p. 167.

La historia

En referencia al análisis hecho en el capítulo primero, en el apartado "La Comunidad de Inteligencia" se explica qué agencias la componen y cómo la mayoría, con excepción de la CIA y la Dirección General de Inteligencia, pertenecen al ramo militar. Aunque antes de la Segunda Guerra Mundial ya existían agencias de Inteligencia, e inclusive la Oficina de Servicios Estratégicos, OSS, es antecesora de la CIA, no fue hasta después de este conflicto que comenzó a forjarse la matriz de lo que ahora reconocemos como un gran complejo de Inteligencia.

La principal actividad de las agencias de Inteligencia es la de brindar información para la toma de decisiones tanto de las fuerzas militares como de los gobiernos en todos los dominios, incluido el espacio cibernético como un nuevo lugar en donde aplicar las fuerzas del complejo tecnológico-militar-industrial y expandir los dominios económicos.

Este apartado deja la sensación del carácter omnipresente de la Inteligencia como sostén del Estado. Si recurriéramos a una metáfora anatómica sobre la estructura estatal, el aparato de Inteligencia serían las piernas que le dan estabilidad al resto del cuerpo. Sin embargo, lo que hoy observamos surge en 1947 con la promulgación de la Ley de Seguridad Nacional, en un momento histórico en el que Europa había sido avasallada por la contienda en su territorio y Estados Unidos se posicionaba como potencia militar.

Pudimos observar, por la información hemerográfica resguardada en el Archivo Gregorio Selser, en el Centro Académico de la Memoria de Nuestra América, Camena; que desde su fundación la NSA se dedica a la vigilancia de las telecomunicaciones, y que de forma paralela se dedicó al espionaje, en ese entonces de los telegramas de las empresas estadunidenses RCA, ITT y Western Union. Porque, en efecto, desde el inicio controlaba las comunicaciones de los ciudadanos. En este marco cabría subrayar que aunque dichas acciones se realizaron en el marco de la guerra, han continuado a lo largo del tiempo. Lo que sufrió modificaciones fue el marco normativo.

El marco jurídico comienza con la Ley de Espionaje de 1917, formulada en principio para expatriar a todos los extranjeros incómodos en la época de la Primera Guerra Mundial y bajo la cual fueron juzgados Daniel Ellsberg, Chelsea Manning y por la hoy se acusa a Edward J. Snowden y a Julian Assange.

La Comunidad de Inteligencia son "todos los departamentos o agencias de un gobierno

involucrados en actividades de Inteligencia. Ya sea en un rol de vigilancia, bien en gestión o con participación directa […]"[436], al entender esto nos acercamos al segundo capítulo: Ciberguerra estadunidense y *Silicon Valley,* en el que comprobamos que las nuevas tecnologías se encuentran en el seno del Estado estadunidense y se congratulan de ello.

¿Complicidad o aparato de Estado?

La alianza Pentágono-Google es explícita. Google entró a la ONU y por medio de -- otra vez-- la democracia, tiene injerencia en países como Irán para "ayudar" a dicho país desde la diplomacia. Así constatamos el uso de armas como Stuxnet y *Flame*. Y aquí surge otra pregunta: ¿es *Silicon Valley* la zanahoria y las armas cibernéticas el garrote en la lucha por la hegemonía estadunidense en el ciberespacio? Recordemos, al respeto, la afirmación de Barack Obama: "La pregunta nunca ha sido si Estados Unidos debe tener o no el liderazgo internacional, la pregunta es cómo".[437]

Asimismo se comprueba que las acciones de vigilancia masiva e interceptación son acompañadas del discurso oficialista de la Seguridad Nacional y la democracia. Empero, con las filtraciones de WikiLeaks la retórica de la diplomacia quedó al descubierto para develar su verdadero uso. Asimismo, con las filtraciones de Snowden las agencias de Inteligencia mostraron su verdadero rostro, sin máscara. El discurso de la Seguridad Nacional quedó, de tal modo, en entredicho.

Pero aún hay otro punto que cuestionar: la falta de memoria y la constante manera de explicar, a botepronto, los sucesos. El escritor pakistaní Tariq Ali nos advierte, en tal sentido, que "uno de los motivos que se esconden tras la pérdida de memoria colectiva en Occidente podría ser resultado de un complejo de superioridad. Ganamos nosotros. Derrotamos al 'imperio del mal'. Somos los mejores. Nuestra cultura, nuestra civilización es infinitamente más avanzada que cualquiera otra […] Uno de los rasgos de la dominación es que aquellas voces, internas o externas, que no se identifican con ella son tildadas de 'el enemigo'. Y eso

[436] *Dod Dictionary of Military and Associated Terms, as of August 2017*, entrada: "intelligence community", p. 114. [traducción propia]
[437] Obama Barack H., The National Security Strategy of the United States of America February 2015, Seal of the President of the United States, p. 3. [traducción propia]

siempre ha sido así. Larga vida a la disidencia."[438]

Podemos concluir que el espionaje sirve a Estados Unidos para garantizar los medios económicos, políticos y militares que aseguren su influencia política, militar-industrial y tecnológica. Pese a todo lo anterior, siempre hay dinámicas de emancipación. La lucha es dura, como lo demuestran los casos de Julian Assange, quien en junio de 2018 cumplió seis años de prisión domiciliaria en la embajada de Ecuador, y de Edward Snowden, al que acorralaron en Rusia y le arrebataron la nacionalidad estadunidense. Estos hechos también demuestran que incluso en las sociedades de la democracia occidental, las cuales argumentan ser justas, hay acciones que se desarrollan al margen de las leyes nacionales, que deberían ser reconocidas como formas de resistencia.

Ante las estrategias de vigilancia y la configuración de sentido siempre existe un contrasentido que da validez a las resistencias. El espacio cibernético es un lugar más de disputa en el que muchos han dado la batalla por su democratización. Tenemos derecho a la privacidad, pero aún más importante es el derecho de hacer uso de las telecomunicaciones como un espacio para construir alternativas. ¿O acaso no sería mejor, y más justa, una red de redes ciudadanizada?

Las aseveraciones anteriores y las conclusiones son arriesgadas, porque no es un tema ni remotamente concluido. Es tan sólo una ventana de duda que surge al aproximarse a las dimensiones del espionaje estadunidense en la actual era tecnológica.

[438] Tariq Ali, "Prólogo", en Vanaik, Achin (ed.), *Casus belli: cómo los Estados Unidos venden la Guerra*, Transnational Institute at Smashwords, 2011, e-book, p. 10.

Línea del tiempo de elaboración propia

Glosario

Algoritmo de encriptación. "[…] Es una función matemática usada en los procesos de encriptación y desencriptación. Trabaja en combinación con una llave (un número, palabra, frase, o contraseña) para encriptar y desencriptar datos. Para encriptar, el algoritmo combina matemáticamente la información a proteger con una llave provista. El resultado de este cálculo son los datos encriptados. Para desencriptar, el algoritmo hace un cálculo combinando los datos encriptados con una llave provista, siendo el resultado de esta combinación los datos desencriptados (exactamente igual a como estaban antes de ser encriptados si se usó la misma llave). Si la llave o los datos son modificados, el algoritmo produce un resultado diferente. El objetivo de un algoritmo criptográfico es hacer tan difícil como sea posible desencriptar los datos sin utilizar la llave."[439]

Aritmética modular. Incluimos este término porque el funcionamiento del Código César se basa en "la aritmética modular o 'aritmética del reloj'. Esta técnica tiene sus orígenes en el trabajo del matemático griego Euclides (325-265 a.C.), y es una de las bases fundamentales de los sistemas modernos de seguridad de la información […]. [...] Los trabajos del matemático griego relativos a la aritmética de operaciones realizadas sobre conjuntos numéricos finitos o *módulos* constituyen uno de los pilares del estudio formal de la criptografía. Conocida y admirada por los árabes, la primera edición europea de las obras de Euclides emergió en Venecia en 1482. Tanto árabes como venecianos fueron […] grandes maestros de la criptografía".[440]

Bit. Es la unidad de medida para cuantificar la información de los sistemas computacionales. Puede representar dos valores: 0 y 1; de aquí surgen las demás combinaciones.

Carrera armamentista. "Fenómeno complejo y mutidimensional que implica tanto la concepción, el diseño, el desarrollo, la producción, la obtención, el

[439] *EcuRed,* en línea, entrada: "algoritmo criptográfico", https://www.ecured.cu/Algoritmo_criptográfico

[440] Joan Gómez Urgellés, *Matemáticos, espías y piratas informáticos. Codificación y criptografía*, [col. El mundo es matemático], España, Impresia Ibérica, National Geographic, 2012, p. 27.

almacenamiento, la transferencia, el despliegue, la prueba y el uso cada vez de más y mejores armas, como el entrenamiento, el equipamiento y la preparación de los ejércitos; se deriva de las acciones unilaterales y recíprocas, frecuentemente en *escalada,* emprendidas en aplicación de políticas decididas para aumentar su *poder* y/o su seguridad, que toman Estados que compiten entre sí, muy especialmente las potencias militares; se da en los ámbitos bilateral y multilateral, regional y mundial; y socava la *Seguridad Nacional*, regional e internacional, pues siempre genera tensiones y conflictos y entraña el riesgo de *guerra,* incluso nuclear."[441]

Certificados de seguridad en Internet. "[…] son una medida de confianza adicional para las personas que visitan y hacen transacciones en su página web […] permite cifrar los datos entre el ordenador y el cliente y el servidor que representa a la página. El significado más preciso […] es que con él logramos que los datos personales sean encriptados y así imposibilitar que sean interceptados por otro usuario".[442]

Cifrar. "El *cifrado* o *cifra*, […] sustituye letras o caracteres. Con el tiempo […] se ha hecho tan prevalente que ha acabado por erigirse en sinónimo de escribir en clave. Si nos atenemos a la precisión anterior, el término correcto para este […] caso sería *encriptar* (y *desencriptar* para el proceso inverso)."[443]

Codificar. "La codificación es un método de escritura en clave que consiste en sustituir unas palabras por otras."[444]

Complejo militar-industrial. "[…] Intelectualmente, la idea se puede concebir desde dos posturas: la sociología política y la economía política. [Nos quedaremos con la visión de la sociología política] La sociología política brinda la idea de élite, en particular la caracterización de C. Wright Mills (1956) acerca de los círculos económico, político y militar en Estados Unidos que forman grupos políticos

---

[441] Hernández-Vela Salgado Edmundo, Diccionario de política internacional, entrada: armamentos, carrera de, Tomo I y II, México, D.F, Porrúa, 2002, p. 31.
[442] s/a, "Certificados de seguridad", Certsuperior en www.certsuperior.com/CertificadosSeguridad.aspx
[443] Joan Gómez Urgellés, *Matemáticos, espías y piratas informáticos. Codificación y criptografía, op. cit.,* p. 10.
[444] *Ídem.*

sobrepuestos. Mills vio que la Guerra Fría tenía una importante conexión causal con la élite en el poder. En este aspecto comparte con los economistas políticos la visión de que 'la permanente economía de guerra' establecida en Estados Unidos después de 1945, creó la infraestructura del complejo militar industrial, [MIC, por sus siglas en inglés]." [445]

Doctrina Carter. "[…En] enero de 1980, en el Discurso del Estado de la Unión, […el presidente Jimmy Carter] declaró que 'cualquier intento de una fuerza exterior para ganar control en la región del Golfo Pérsico será considerada una agresión a los intereses vitales de Estados Unidos, y que dicha agresión será rechazada por cualquier medio necesario, incluyendo la fuerza militar'. El discurso fue una respuesta directa a los acontecimientos en Irán en 1979 (la caída del Shah y su reemplazo por el Ayatolá Jomeini) y la invasión soviética a Afganistán en el mismo año. Estos dos eventos fueron percibidos como amenazas a los intereses vitales de Estados Unidos en la región del Golfo. Tuvo como motivación principal el acceso al petróleo y las ventajas estratégicas."[446]

Doctrina Clinton. "Como el primer presidente estadunidense de la Posguerra Fría, Bill Clinton estaba ansioso […] de establecer su propia doctrina de política exterior […] De acuerdo a la Estrategia de Seguridad Nacional de 1994, titulada *Una estrategia para el compromiso y la ampliación*[447], documento que prevalece como la clara articulación de los imperativos de la política exterior para el milenio, la Estrategia de Seguridad Nacional se basa en tres pilares: retención de la predominancia militar global, la búsqueda de una continua prosperidad económica y la promoción de la democracia de mercado en el extranjero. A diferencia de la [política] de la contención y […] la disuasión durante la Guerra Fría, esta nueva directriz política no implica un ilimitado compromiso con la intervención militar."[448]

---

[445] Graham Evans, Newnham Jeffrey, *Dictionary of International Relations*, entrada: military-industrial complex, Londres, p. 326. [traducción propia]
[446] *Ibíd.,* pp. 61-62.
[447] En inglés: *A Strategy for Engagement and Enlargement*.
[448] Graham Evans, Newnham Jeffrey, *Dictionary of International Relations*, entrada: Clinton Doctrine, p. 68.

Doctrina Eisenhower. "[…] resolución conjunta del Congreso en 1957 […] que autorizó al presidente [Eisenhower] para asistir a cualquier Estado de Medio Oriente amenazado por una agresión comunista. Aunque supuestamente se dirigió contra la propagación del comunismo internacional, esta doctrina fue un intento específico para limitar [… el margen de acción] del presidente Nasser en Egipto. Bajo los términos de la resolución se podían enviar fuerzas militares de Estados Unidos o ayuda económica bajo el Programa de Seguridad Mutua".[449] [450]

Doctrina Nixon. "Originalmente concebida como Doctrina Guam desde que su primer esbozo se articuló en una serie de declaraciones informales en Guam, Filipinas en julio de 1969. […] De acuerdo con Henry Kissinger, la declaración del presidente [Nixon] del 3 de noviembre de 1969 sobre Vietnam deliberadamente volvió a estos temas para asegurarse que la doctrina se nombrara como el presidente. […] En esencia, esta doctrina contiene tres asuntos fundamentales de políticas: 1. Se comprometía a que Estados Unidos conservaría todos los compromisos contraídos; 2. Prometía 'proveer un escudo' si un poder nuclear amenazaba a un aliado o a cualquier otro Estado cuya supervivencia se estimara importante para los intereses de Estados Unidos, [y] 3. En caso de agresiones no nucleares, Estados Unidos se compromete a proveer ayuda militar y económica con la condición de que 'veamos a la nación directamente amenazada para asumir la primordial responsabilidad de prestación de recursos humanos para su defensa."[451]

Geoestrategia: "[…] la gestión estratégica de los intereses geopolíticos".[452]

Guerra Fría. No corresponde al estudio específico de esta tesis elaborar un análisis profundo del periodo considerado como Guerra Fría. Sin embargo, es necesario tener una idea de él en relación con las agencias de Inteligencia. Señalemos, por

---

[traducción propia]

[449] En inglés: *Mutual Security Programme.*

[450] Graham Evans, Newnham Jeffrey, *Dictionary of International Relations*, entrada: Eisenhower Doctrine, p. 146.

[451] Graham Evans, Newnham Jeffrey, *Dictionary of International Relations*, entrada: Nixon Doctrine, pp. 373-374. [traducción propia]

[452] Zbigniew Brzezinski, "Capítulo 1. Una nueva clase de hegemonía", *El gran tablero mundial. La supremacía estadunidense y sus imperativos geoestratégicos*, s/c, Paidós, s/año, pp. 11 y 12.

consiguiente, que "dentro de la visión occidental (sobre la *Guerra Fría)* destaca la que se considera como aquella en la que las controversias internacionales no se intentan arreglar por medios militares, sino a través de presiones políticas, económicas o propagandísticas, que encierran, en forma oculta o manifiesta, una amenaza militar para doblegar al contrario'. De igual forma, en la perspectiva soviética la *Guerra Fría* era considerada como la reacción occidental desencadenada por el triunfo de la Revolución Socialista, que agudizó la lucha ideológica entablada entre los países capitalistas y la Unión Soviética."[453]

Guerra preventiva. "El discurso del presidente Bush del 29 de enero de 2002 […] puso de manifiesto que la administración estadunidense abandonaba la justificación de la legítima defensa y adoptaba, unilateralmente, la doctrina de la guerra preventiva o 'preemptive war' como Estrategia de Seguridad Nacional *(National Security Strategy).*"[454]

Gusano o virus informático. "[…] es un programa de software malicioso que puede replicarse a sí mismo en ordenadores o a través de redes de ordenadores sin que el usuario se dé cuenta que el equipo está infectado. Como cada copia del virus o gusano informático, también puede reproducirse, (pues) las infecciones pueden propagarse de forma muy rápida. Existen muchos tipos diferentes de virus y gusanos informáticos, y muchos de ellos pueden provocar grandes niveles de destrucción".[455]

Información clasificada. Se toma la definición que utiliza el Departamento de Defensa para comprender qué entienden las agencias de Inteligencia bajo esta denominación. "Información oficial solicitada que requiera, en el interés de la Seguridad Nacional, protección contra divulgaciones no autorizadas por lo que ha sido designada bajo esa clasificación."[456]

---

[453] Hernández-Vela Salgado Edmundo, Diccionario de política internacional, entrada: Guerra fría, Tomo I y II, México, D.F, Porrúa, 2002, p. 31.
[454] Caro Garzón, Octavio Augusto, "La doctrina Bush en la guerra preventiva: ¿Evolución del 'ius ad bellum' o vuelta al Medievo?, *op.cit.,* p. 420.
[455] s/a, "Virus y gusanos informáticos", Kaspersky Lab, en https://www.kaspersky.es/resource-center/threats/viruses-worms
[456] *Dod Dictionary of Military and Associated Terms, as of August 2017*, entrada: classified information, p. 35. [traducción propia]

Llave pública y llave privada. "A través de un juego entre distintos caracteres informáticos la llave pública solamente puede cifrar. La llave privada puede descifrar o hacer las dos cosas, aunque esto último no es tan importante. Se recibe la llave pública del destinatario y con ella cifra la información que se le enviará. Una vez cifrada, no se puede ver la información. Al enviarla, en un correo por ejemplo, el destinatario la recibe y la descifra con su llave privada. Es por ello que las llaves permiten a los usuarios acreditarse frente a otros usuarios y usar la información de los certificados de identidad (por ejemplo, las claves públicas de otros usuarios) para cifrar y descifrar mensajes, firmar digitalmente información, garantizar el no repudio de un envío […]".[457]

***Malware*.** "[…] (Abreviatura de 'software malicioso'). Se considera un tipo molesto o dañino de software destinado a acceder a un dispositivo de forma inadvertida, sin el conocimiento del usuario. Los tipos de *malware* incluyen spyware (software espía), adware (software publicitario), phishing, virus, troyanos, gusanos, rootkits, ransomware y secuestradores del navegador."[458]

Metadata telefónica. "La información que incluye los números de teléfono tanto de los que originan las llamadas como de quien la recibe, el tiempo de llamada y la fecha de la misma". [459]

Panóptico. Modelo de centro penitenciario concebido por el filósofo Jeremy Bentham en 1978 con el fin de que un solo vigilante pudiera espiar, al mismo tiempo, a todos los prisioneros, al estar todos en su mismo campo visual.[460] En sentido figurado, se utiliza el concepto de panóptico como analogía a la capacidad de vigilancia absoluta, en general en referencia al poder en manos del Estado.

---

[457] s/a, "Llave pública y llave privada. ¿Qué son y cómo funcionan?, Certsuperior. Blog de seguridad informática, en https://www.certsuperior.com/Blog/llave-publica-y-llave-privada-que-son-y-como-funcionan

[458] s/a, "*Malware* y Anti*malware*", Avast, en https://www.avast.com/es-es/c-*malware*

[459] Richard A. Clarke, Michael J. Morell, Geoffrey R. Stone, Cass R. Sunstein y Peter Swire, "Liberty and Security in a Changing World. Report and Recommendations of The President´s Review Group on Intelligence and Communications Technologies", 13 de diciembre de 2013, https://obamawhitehouse.archives.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf, p. 17.

[460] Julian Assange, María Maestro (trad.), *Cypherpunks. La libertad y el futuro de Internet*, *op.cit.,* p.45.

Proyecto Manhattan. "El nombre en código del proyecto para construir una bomba atómica en agosto de 1942. La investigación científica después de esto, cayó bajo la tutela del control político y militar del gobierno de Estados Unidos. Las reglas de la investigación académica se abandonaron y la más rigurosa secrecía prevaleció. El hecho de que el proyecto fue liderado por el general Leslie Richard Groves, es indicativo de la primacía militar/securitaria sobre los cánones de la ciencia en la academia."[461]

Software. "En informática, conjunto de instrucciones y datos regulados para ser leídas e interpretadas por una computadora. Estas instrucciones y datos fueron concebidos para el procesamiento electrónico de datos".[462]

Software libre. "[…] se refiere a la libertad de los usuarios para ejecutar, copiar, distribuir, estudiar, cambiar y mejorar el software. De modo más preciso se refiere a cuatro libertades de los usuarios del software: 1. Libertad de usar el programa con cualquier propósito (libertad 0); 2. Libertad de estudiar cómo funciona el programa y adaptarlo a tus necesidades (libertad 1). […]; 3. Libertad de distribuir copias […] (libertad 2) y 4. Libertad de mejorar el programa y hacer públicas las mejoras a los demás, de modo que toda la comunidad se beneficie (libertad 3)."[463]

Tecnotrónica y Soft power. "[…] desde finales de los años 1960, el geopolitólogo estadunidense de origen polaco, Zbigniew Brzezinski, especialista en estudios sobre comunismo y futuro consejero de James Carter en materia de Seguridad Nacional, había ofrecido la última clave de la vía hacia un mundo basado en la gestión de las tecnologías de la información. Idea que desarrolló en sus análisis en torno de las implicaciones internacionales de la convergencia entre la informática, las técnicas audiovisuales y las telecomunicaciones. […] su obra sobre la revolución tecnotrónica, publicada en 1969, deber ser leída como el remate de los discursos sobre los finales, en un intento de formulación de una estrategia de hegemonía

[461] Graham Evans, Newnham Jeffrey, *Dictionary of International Relations*, entrada: Manhattan Project, p. 313. [traducción propia]
[462] s/a, "Software", EcuRed, en https://www.ecured.cu/Software
[463] s/a, "¿Qué es el software libre?", HispaLinux, hacia la sociedad del conocimiento libre, http://hispalinux.es/softwarelibre

mundial. […] Lo que hay que demostrar a toda costa [según esta postura] es que las relaciones imperiales han muerto y que, de forma natural, se ha instaurado una única opción universalista. La diplomacia de las redes ha vencido a la diplomacia del canon. Un cuarto de siglo más tarde, los estrategas de la administración Clinton retomarán este argumento mediante la doctrina del *soft power*. La idea es que el poder de expansión de la web, junto a la seducción de la democracia estadunidense y las virtudes de los mercados libres, fundan una nueva diplomacia". [464]

[464] Armand Mattelart y André Vitalis, Juan Carlos Miguel de Bustos (trad.), *De Orwell al cibercontrol*, *op. cit.,* pp. 85 y 86.

Fuentes consultadas

Bibliografía

Abbagnano, Nicola, Pedro Torres Aguilar (rev.), José Esteban Calderón *et al.* (trad.), *Diccionario de filosofía. Actualizado y aumentado por Giovanni Fornero/Nicola Abbagnano,* México, D.F., Fondo de Cultura Económica, 2004, 1103 pp.

Assange Julian, Iván Barbeitos García (trad.), *Cuando Google encontró a WikiLeaks,* Ciudad Autónoma de Buenos Aires, Capital Intelectual, 2014, 240 pp.

Assange Julian, María Maestro (trad.), *Cypherpunks. La libertad y el futuro de Internet*, México, D.F., Planeta Mexicana, 2013, 222 pp.

Berman Morris, Eduardo Rabasa (trad.), *Edad oscura americana. La fase final del imperio*, Madrid, Sexto Piso, 2008, 505 pp.

Bobbio Norberto, Nicola Matteucci y Gianfranco Pasquino (bajo la dirección de), Raúl Crisafo, et.al.(trad.), *Diccionario de política,* Edo. de México, Siglo XXI, 2008, volumen I de la a a la j, 852 pp.

Brzezinski Zbigniew, "Capítulo 1. Una nueva clase de hegemonía", *El gran tablero mundial. La supremacía estadunidense y sus imperativos geoestratégicos*, s/c, Paidós, s/año, pp. 11-39

Castells Manuel, María Hernández (trad.), C*omunicación y poder*, Madrid, Alianza Editorial, 2009, 667 pp.

Clarke Richard A., Robert K. Knake, Luis Alfonso Noriega (trad.), *Guerra en la red. Los nuevos campos de batalla,* Barcelona, Ariel, 2011, 367 pp.

Chomsky Noam, Morgenthau Hans, Manuela Díez (trad.), *El interés nacional y los documentos del Pentágono,* Barcelona, a. redondo, editor, 1973, 73 pp.

Evans Graham, Newnham Jeffrey, *Dictionary of International Relations,* Londres, Penguin Books, 1998, 623 pp.

Flichy Patrice, Eugeni Rosell i Miralles (trad.) *Una historia de la comunicación moderna. Espacio público y vida privada*, San Adrián de Besós, G. Gili, 1993, 260 pp.

Gómez Urgellés Joan, *Matemáticos, espías y piratas informáticos. Codificación y criptografía,* [col. El mundo es matemático], España, Impresia Ibérica, National Geographic, 2012, 142 pp.

Hernández-Vela Salgado Edmundo, *Diccionario de política internacional,* Tomo I y II, México, D.F, Porrúa, 2002, 1295 pp.

Lefébure Antoine, Bárbara Poey Sowerby (trad.), *El caso Snowden. Así espía Estados Unidos al mundo*, [col.] *Le Monde diplomatique*, Ciudad Autónoma de Buenos Aires, Capital intelectual, 2014, 368 pp.

Leigh David, Harding Luke, Mar Vidal e Isabel Merino (trad.), *WikiLeaks y Assange. Un relato trepidante sobre cómo se fraguó la mayor filtración de la historia,* México, D.F, Planeta Mexicana, 2011, 275 pp.

Loya Sergio, *Manual de estilo Proceso*, México, D.F, Proceso y Random House Mondadori, 2010, 196 pp.

Mattelart Armand, Gilles Multigner (trad.), *Historia de la sociedad de la información*, Barcelona, Paidós, 2002, 192 pp.

Mattelart Armand, Gilles Multigner (trad.), *Un mundo vigilado,* Barcelona, Paidós, 2009, 284 pp.

Mattelart Armand y Vitalis André, Juan Carlos Miguel de Bustos (trad.), *De Orwell al cibercontrol,* Barcelona, Gedisa, 2015, 228 pp.

Mills C. Wright, Florentino M. Turner, Ernestina de Champourcin (trad.), *La élite del poder,* México, D.F., Fondo de Cultura Económica, 1973, 388 pp.

Sanger David E., *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power*, Nueva York, Random House, 2012, e-book, 438 pp.

Serge Victor, Daniel Molina (trad.), *Lo que todo revolucionario debe saber sobre la represión,* [Serie popular Era/16], México, D.F., Era, 1972, 141 pp.

Sun Tzu, *El arte de la guerra*, Estado de México, Casa editorial Boek México, s/ año, 99 pp.

s/a, *Diccionario de sinónimos y antónimos,* Editorial Gredos, España, 2009, s/ número de páginas.

s/autor, *Dod Dictionary of Military and Associated Terms,* as of August 2017.

s/a, *Intelligence Community Legal Reference Book,* Office of the Director of National Intelligence, Office of General Counsel, Summer 2016, 1023 pp.

Vanaik, Achin (ed.), Casus belli: cómo los Estados Unidos venden la Guerra, Transnational Institute at Smashwords, 2011, e-book, 371 pp.

Widemer Ted, *American speeches. Political oratory from Patrick Henry to Barack Obama*, [col. Library of America], Nueva York, Penguin Random House, , 2011, 403 pp.

Zetter Kim, *Countdown to Zero Day. Stuxnet and the launch of the world's first digital weapon,* Nueva York, Penguin Random House Company, 2014, 265 pp.

Zinn Howard, Toni Strubel (trad.), *La otra historia de los Estados Unidos (desde 1492 hasta hoy)*, México, D.F., Siglo XXI, 2010, 519 pp.

Artículos

Aid, Matthew M., William Burr, "Secret Cold War Documents Reveal NSA Spied on Senators...along with Muhammad Ali, Martin Luther King, and a Washington Post humorist", Investigation, Foreign Policy, 25 de septiembre de 2014, http://foreignpolicy.com/2013/09/25/secret-cold-war-documents-reveal-nsa-spied-on-senators/

Broad, William J., John Markoff y David E. Sanger, "Israeli Test on Worm Called Crucial in Iran Nuclear Delay", Middle East, The New York Times, 15 de enero de 2011, https://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html

Bronk, Chris, "Cyber Intrigue: The *Flame Malware* International Politics", Munk School of Global Affairs, The University of Toronto, 31 de mayo de 2012, http://www.cyberdialogue.ca/2012/05/cyber-intrigue-the-*Flame-malware*-international-politics/

Campbell, Duncan, "Thatcher Bugged by her 'closest ally", BBC Newsright, 25 de julio de 1980, 1 pp.http://www.duncancampbell.org/menu/journalism/newstatesman/newstatesman-1980/Thatcher%20Bugged%20by%20her%20Closest%20Ally.pdf [traducción propia]

Campbell, Duncan, "Threat of the electronic spies", New Statesman, 2 de febrero de 1979, pp. 142-145.

Duncan Campbell y Linda Mervin, "America´s big ear in Europe", New Statesman, 18 de julio de 1980, pp. 10-14. [traducción propia] http://www.duncancampbell.org/PDF/America's%20Big%20Ear%20on%20Europe%2018%20July%201980.pdf

Campbell, Duncan, y Mark Hosenball, "The eavesdroppers", Time Out, No. 21-27 de mayo de 1976, http://www.duncancampbell.org/menu/journalism/timeout/Eavesdroppers.pdf

Caro Garzón, Octavio Augusto, "La doctrina Bush en la guerra preventiva: ¿Evolución del 'ius ad bellum' o vuelta al Medioevo?", Revista FACULTAD DE DERECHO Y CIENCIAS POLÍTICAS, Vol. 36, No. 105, Medellín-Colombia, Julio-Diciembre de 2016, pp. 399-429.

Child, Ben, "Citizenfour director Laura Poitras sues US over 'Kafkaesque harassment'", The Guardian, 14 de julio de 2015, https://www.theguardian.com/film/2015/jul/14/citizenfour-director-laura-poitras-sues-us-harassment-edward-snowden

Davies Nick, David Leigh, “Afghanistan war logs: Massive leak of secret files exposes truth of occupation”, The Guardian, 25 julio de 2010, en https://www.theguardian.com/world/2010/jul/25/afghanistan-war-logs-military-leaks

Davies Nick, Jonathan Steele y David Leigh, “Iraq war logs: secret files show how US ignored torture”, The Guardian, 22 de octubre de 2010, https://www.theguardian.com/world/2010/oct/22/iraq-war-logs-military-leaks

DeCarlo, Scott, “Fortune 500”, Fortune, 2017, http://fortune.com/fortune500/

Estrada Corona, Adrián, “Protocolos TCP/IP de Internet”, Revista Digital Universitaria, Vol. 5, No. 8, 10 de septiembre de 2004, DGSCA-UNAM, 7 pp.

Farrell, Paul, “History of 5-Eyes-explainer”, The Guardian, International edition, Lunes 2 de diciembre de 2013, http://www.theguardian.com/world/2013/dec/02/history-of-5-eyes-explainer

Gady, Franz-Stefan, “Undersea Cables: How Russia Targets the West’s Soft Underbelly”, The Diplomat. Read the Diplomat, Know the Asia-Pacififc, 27 de octubre de 2015, https://thediplomat.com/2015/10/undersea-cables-how-russia-targets-the-wests-soft-underbelly/

Gellman, Barto, y Ashkan Soltani, “NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say”, The Washington Post, 30 de noviembre de 2013, www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html?utm_term=.1318336f846d

Gilder, George, “The Information Factories”, Wired, 10 de enero 2006, https://www.wired.com/2006/10/cloudware/ [traducción propia]

Greenwald, Glenn, “NSA collecting phone records of millions of Verizon customers daily”, The Guardian, 6 de junio de 2013, https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order

Gostev, Alexander, “The *Flame*: Questions and Answers”, Incidents, Secure List, 20 de mayo de 2012, https://securelist.com/the-*Flame*-questions-and-answers-51/34344/

Kedmey, Dan, “What’s next for Snowden: 10 notorious leakers and how they fared”, Time, 10 de junio de 2013, http://world.time.com/2013/06/10/10-notorious-leakers-and-how-they-fared/slide/daniel-ellsberg/

Kemp, Simon, “Digital in 2017. Global Overview. A collection of Internet, social media and mobile data from around the world”, Special reports, we are social, 24 de enero de 2017, https://wearesocial.com/special-reports/digital-in-2017-global-overview

Kiriakou, John, “The US Postal Service Is Spying on Us”, Reader Supported News, 30 de noviembre de 2015, http://readersupportednews.org/opinion2/277-75/33772-the-us-postal-service-is-spying-on-us

Lee, Tomothy B., “40 maps that explain the Internet”, Vox, junio de 2014, https://www.vox.com/a/Internet-maps

Leigh, David, “US embasy cable leak sparks global diplomatc crisis”, The US embasy cables, The Guardian, Sun 28 Nov 2010, https://www.theguardian.com/world/2010/nov/28/us-embassy-cable-leak-diplomacy-crisis

Lenzner, Robert, “AT&T, Verizon, Sprint are paid cash by NSA for your private communications”, Forbes, 23 de septiembre de 2013,

http://www.forbes.com/sites/robertlenzner/2013/09/23/attverizonsprint-are-paid-cash-by-nsa-for-your-private-communications/#34d562341f15

Levy, Steven, "Crypto Rebel", Wired, 2 enero de 1993, https://www.wired.com/1993/02/crypto-rebels/

Linder, Douglas O., "The Pentagon Papers (Daniel Ellsberg) Trial: An Account", Famous Trials, s/fecha, www.famous-trials.com/ellsberg/273-home

Lozano, Víctor Miguel, "El uso de códigos secretos y el derecho a la privacia", unomásuno, 19 de septiembre de 1981 en Gregorio Selser, NSC: National Security Council. NSA: National Security Agency. Agencias de Inteligencia militares de los Estados Unidos. 1960-1990, Fondo A, Recortes y páginas de diarios, páginas de revistas, cables, Clave Expediente:W US99, imagen 27/99, CAMENA, UACM.

MacAskill, Ewen, Julian Borger, Nick hopkins, Nick Davies y James Ball, "GCHQ taps fibre-optic cables for secret acces to world's communications", The Guardian, 21 de junio de 2013, http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa

Malcomson, Scott, "Welcome to the SplInternet", The World Post, 21 de diciembre de 2015,http://www.huffingtonpost.com/scott-malcomson/welcome-to-the splinterne_b_8855212.html [traducción propia]

Nakashima, Ellen, "A Story of Surveillance", Washington Post, 7 de noviembre de 2007, http://www.washingtonpost.com/wpdyn/content/article/2007/11/07/AR2007110700006.html

Perrone, Jane, "The Echelon spy network", The Guardian, International edition, 29 de mayo de 2001, http://www.theguardian.com/world/2001/may/29/qanda.janeperrone

Savage, Charlie, “Classification Guide for Stellarwid Program”, The New York Times, 11 de marzo de 2014, https://www.nytimes.com/interactive/2014/03/12/us/stellarwind-guidance-doc.html

Shalal, Andrea, “Former Google CEO Schmidt to head new Pentagon innovation board”, Reuters, 2 de marzo de 2016, http://www.reuters.com/article/us-usa-military-innovation-idUSKCN0W421V

Shane, Scott, y Andrew W. Lehren, “Leaked Cables Offer Raw Look at U.S Diplomacy”, Mundo, The New York Times, 28 de noviembre de 2010, https://www.nytimes.com/2010/11/29/world/29cables.html

Sheehan, Neil “Vietnam Archive: Pentagon Study Traces 3 Decades of Growing U. S Involvement”, New York Achives/ 1971, The New York Times, 13 de junio de 1971, https://www.nytimes.com/1971/06/13/archives/vietnam-archive-pentagon-study-traces-3-decades-of-growing-u-s.html [traducción propia]

Smith, Dave, “Take a look at Facebook´s gorgeous data centers from around the world”, Business Insider, 16 de febrero de 2017, http://www.businessinsider.com/facebook-data-centers-photos-2017-2/#heres-a-look-inside-facebooks-data-center-in-forest-city-north-carolina-the-company-launched-this-center-in-2010-1

Sterne, Peter, “How the Espionage Act morphed into a dangerous tool used to prosecute sources and threaten journalists”, II/III, Freedom of the Press Foundation, 19 de junio de 2017, https://freedom.press/news/how-espionage-act-morphed-dangerous-tool-used-prosecute-sources-and-threaten-journalists/

s/a, “Certificados de seguridad”, Certsuperior en www.certsuperior.com/CertificadosSeguridad.aspx

s/a, “Facebook officially announces massive Sarpy, Nebraska data center”; News Roundup, Data Center of the World, DCD Magazine, Data Center Dynamics, Londres, Abril/Mayo 2017, p. 8.

s/a, “Google announces three new cloud regions: California, Montreal and Netherlands”, News Roundup, Data Center of the World, DCD Magazine, Data Center Dynamics, Londres, Abril/Mayo 2017, p. 9.

s/a, “History of FOIA”, Electronic Frontier Foundation, https://www.eff.org/es/issues/transparency/history-of-foia [traducción propia]

s/a, “Internet usage statistics. The Internet big picture. World Internet Users and 2018 Population Stats”, Miniwatts Marketing Group, https://www.Internetworldstats.com/stats.htm

s/a, “Inside Somalia and the Union of Islamic Courts”, WikiLeaks, diciembre de 2006,https://WikiLeaks.org/wiki/Inside_Somalia_and_the_Union_of_Islamic_Courts

s/a, “Letters between WikiLeaks and the U.S Government”, The New York Times, s/f, https://www.nytimes.com/interactive/projects/documents/letters-between-WikiLeaks-and-gov#document/p5

s/a, “Llave pública y llave privada. ¿Qué son y cómo funcionan?, Certsuperior. Blog de seguridad informática, en https://www.certsuperior.com/Blog/llave-publica-y-llave-privada-que-son-y-como-funcionan

s/a, “*Malware* y Anti*malware*”, Avast, en https://www.avast.com/es-es/c-*malware*

s/a, “Medio mundo estará en línea en 2017”, All News, Unesco, https://es.unesco.org/news/medio-mundo-estará-línea-2017

s/a, “NSA slides explain the PRISM data-collection program”, The Washington Post, abril de 2013 http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/

s/a,“Pentagon whistleblower Daniel Ellsberg: Julian Assange is not a terrorist”, Democracy Now, 12 de octubre de 2010, www.huffingtonpost.com/democracy-now/pentagon-whistleblower-da_b_795045.html

s/a, “¿Qué es el software libre?”, HispaLinux, hacia la sociedad del conocimiento libre, http://hispalinux.es/softwarelibre

s/a, “Stats”, Company info, Newsroom, Facebook, https://newsroom.fb.com/company-info

s/a, “The Facebook Data Center FAQ”, Data Center Knowledge, http://www.datacenterknowledge.com/data-center-faqs/facebook-data-center-faq

s/a, “The evolution of de U.S. Intelligence Community-An Historical Overview”, Federation of American Scientists, http://fas.org/irp/offdocs/int022.html#fnt7

s/a, “The people behind Google”, Google Company, www.google.com/about/company/facts/

s/a, “U.S. vs. Edward J. Snowden criminal complaint”, The Washington Post, https://apps.washingtonpost.com/g/documents/world/us-vs-edward-j-snowden-criminal-complaint/496/

s/a, “Virus y gusanos informáticos”, Kaspersky Lab, en https://www.kaspersky.es/resource-center/threats/viruses-worms

“What is WikiLeaks”, 3 de noviembre de 2015 en https://WikiLeaks.org/What-is-WikiLeaks.html

Whiteclay Chambers II, Dr. John, "Office of Strategic Services Training During World War II", Training for War and Espionage, *Studies in Intelligence Vol. 54, No. 2 (June 2010)*, www.cia.gov/library/readingroom

Winning, Andrew, "WikiLeaks founder Julian Assange at press conference, 2010", Reuters/Landov, https://www.britannica.com/topic/WikiLeaks

Wong, Katherine L., "Recent Developments. The NSA Terrorist Surveillance Program", Harvard Journal on Legislation, 2006, Vol. 43, No. 2, pp.517-534.

Zetter, Kim, "Researchers connect *Flame* to US-Israel Stuxnet attack", Wired, 6 noviembre de 2012, https://www.wired.com/2012/06/*Flame*-tied-to-stuxnet

Fuentes Hemerográficas

Data Center of the World, DCD Magazine, Data Center Dynamics, Londres, Abril/Mayo 2017, 64 pp.

Elola, Joseba, "Entrevista a Evgeny Morozov", El País Semanal: Las mil y un caras de la locura, Madrid, domingo 20 de diciembre de 2015, pp. 28-32.

Jorge Sánchez Cordero, "La figura del informante. El mito de Apolo y Coronis"; Proceso, No. 2152, 21 de enero de 2018.

s/a, con información de AFP, DPA, Reuters, PL y The Independent, "Con los archivos se muestra la verdad el baño de sangre en Irak´: WikiLeaks", La Jornada, Mundo, domingo 24 de octubre de 2010, p. 24.

Documentos

Artículo 51, "Capítulo VII: Acción en caso de amenazas a la paz, quebrantamientos de la paz o actos de agresión", *Carta de Naciones Unidas*, en http://www.un.org/es/sections/un-charter/chapter-vii/index.html

Bazan, Elizabeth B., Legislative Attorney, American Law Division, *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. Updated February 15, 2007*, CRS Report for Congress, Prepared for Members and Committes of Congress, Congressional Research Service.

Bush George W., *The National Security Strategy of the United States of America September 2002,* Seal of the President of the United States.

"Camp Delta Standard Operating Procedure", WikiLeaks, 7 noviembre de 2007, en https://WikiLeaks.org/wiki/Camp_Delta_Standard_Operating_Procedure

"Church of Scientology collected Operating Thetan documents"; WikiLeaks, 8 de marzo de 2008, en https://WikiLeaks.org/wiki/Church_of_Scientology_collected_Operating_Thetan_documents

Clarke, Richard A., Michael J. Morell, Geoffrey R. Stone, Cass R. Sunstein y Peter Swire, *Liberty and Security in a Changing World. Report and Recommendations of The President´s Review Group on Intelligence and Communications Technologies*, 13 de diciembre de 2013, https://obamawhitehouse.archives.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf

"Climatic Research Unit emails, data, models, 1996-2009", WikiLeaks, 21 de noviembre de 2009, en https://WikiLeaks.org/wiki/Climatic_Research_Unit_emails,_data,_models,_1996-2009

"CIA: Agencia Central de Inteligencia de los Estados Unidos 1958", CAMENA, Fondo A, Año de publicación 1958, Clave del expediente W US5, recortes y páginas de diarios, páginas de revistas y cables, fuente: Gregorio Selser. pp. 15 y 16.

Declaración Universal de Derechos Humanos, Yacine Ait Kaci (ilustraciones), Naciones Unidas, 2015.

Electronic Freedom of Information Act Amendments of 1996, United States Department of Justice, https://www.justice.gov/oip/electronic-freedom-information-act-amendments-1996 [traducción propia]

Hughes, Eric, *A Cypherpunk´s Manifesto*, Electronic Frontier Foundation, 9 de marzo de 1993, https://w2.eff.org/Privacy/Crypto/Crypto_misc/cypherpunk.manifesto [traducción propia]

"Iraq & Afghan War Diaries", War Diaries, WikiLeaks, en https://wardiaries.WikiLeaks.org

May, Tim C., *The Crypto Anarchist Manifiesto*, activism.net/cypherpunk/

Pacto Internacional de Derechos Civiles y Políticos, Naciones Unidas, Derechos Humanos, Oficina del Alto Comisionado, Adoptado y abierto a la firma, ratificación y adhesión por la Asamblea General en su resolución 2200 A (XXI), de 16 de diciembre de 1966, en https://www.ohchr.org/sp/professionalinterest/pages/ccpr.aspx

"Plus D. Public Library of US Diplomacy", WikiLeaks, https://WikiLeaks.org/plusd/

Protect America Act of 2007, 121 STAT. 552. PUBLIC LAW 110-55- 110th Congress, https://www.gpo.gov/fdsys/pkg/STATUTE-121/pdf/STATUTE-121-Pg552.pdf [traducción propia]

Selim, Jahan, (director y autor principal), *Panorama general. Informe sobre Desarrollo Humano 2015. Trabajo al servicio del desarrollo humano*, Publicado por el Programa de las Naciones Unidas para el Desarrollo (PNUD), http://www.un.org/es/publications/publipl225.shtml

U.S. Code, Title 50, Capter 15, Subchapter I, sección 403-5d", https://www.law.cornell.edu/uscode/text/50/403–5d [traducción propia]

Obama Barack H., *The National Security Strategy of the United States of America May* 2010, Seal of the President of the United States, 60 pp.

Obama Barack H., *The National Security Strategy of the United States of America February* 2015, Seal of the President of the United States, 35 pp.

Rodham Clinton, Hillary "Remarks on Internet Freedom", Electronic Frontier Foundation, martes 15 de febrero de 2011.

The Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), Privacy & Civil Liberties, Justice Information Sharing, https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1282

The Global Intelligence Files, WikiLeaks, search.WikiLeaks.org/gifiles/?viewemailid=1121800

"Country Clearance Granted for Jared Cohen to meet with ASG BOB ORR", *Public Library of Us Diplomacy,* WikiLeaks, telegram (cable), Canonical ID: 08USUNNEWYORK489_a, 3 de junio de 2008, WikiLeaks.org/plusd/cables/08USUNNEWYORK489_a.htm

"How the NSA Attacks Tor/Firefox Users With Quantum and FOXACID", Email-ID 66482, 2013-10-08, de d.vincenzetti@hackingteam.com, para: list@hackingteam.it, *Hacking Team* Archive, WikiLeaks, https://WikiLeaks.org/hackingteam/emails/emailid/66482

"Researchers Connect *Flame* to US-Israel Stuxnet Attack", Email-ID 598638, 2012-06-12, De: vince@hackingteam.it, para list@hackingteam.it, *Hacking Team* Archive, WikiLeaks, https://WikiLeaks.org/hackingteam/emails/emailid/598638

"*Re: Google & Iran **internal use only -pls do not forward**",* Email-ID 1121800, 2011-02-27, de: burton@strartfor.com, para: scott.stewart@stratfor.com, secure@stratfor.com, The GiFiles, WikiLeaks, search.WikiLeaks.org/gifiles/?viewemailid=1121800

"War Diaries", WikiLeaks, https://WikiLeaks.org/irq/

Filmografía

Aristegui, Carmen, "Chomsky advierte sobre Google y Facebook", Aristegui, CNN, 21 de noviembre de 2017, https://www.youtube.com/watch?v=poJ5Q2tX0bU

Aristegui, Carmen, "Chomsky. El riesgo de una guerra nuclear", Aristegui, CNN, 22 de noviembre de 2017, https://www.youtube.com/watch?v=G0I8lJdg5to

Assange, Julian, "Cypherpunks" parte 1 y 2, *The Julian Assange Show*, Russia Today, 5 de junio del 2012, https://www.youtube.com/watch?v=eil_1j72LOA

Collateral Murder, WikiLeaks, Irak, en https://collateralmurder.WikiLeaks.org

Complete Obama Press Conference on NSA Surveillance, Snowden & US-Russia Relations", August 9, 2013", Youtube, https://www.youtube.com/watch?v=paZgOC7Wqo0

Ehrlich, Judith, Goldsmith Rick, *The most dangerous man in America. Daniel Ellsberg and the Pentagon Papers,* First Run Features, Estados Unidos, 2009, 93 minutos.

Poitras, Laura, *Citizenfour*, Praxis Films, Participant Media, HBO Films, Estados Unidos, Alemania, 2014, 144 minutos.

Poitras, Laura, Glenn Greenwald, "NSA whistleblower Edward Snowden: 'I don´t want to live in a society that does these sort of things'", The NSA files, The Guardian, 9 de junio de 2013, https://www.theguardian.com/world/video/2013/jun/09/nsa-whistleblower-edward-snowden-interview-video

s/a, "Complete Obama Press Conference on NSA Surveillance, Snowden & US-Russia Relations- August 9, 2013", Youtube, https://www.youtube.com/watch?v=paZgOC7Wqo0

s/a, "*Malware* y Anti*malware*", Avast, en https://www.avast.com/es-es/c-*malware*

s/a, "Pentagon whistleblower Daniel Ellsberg: Julian Assange is not a terrorist", Democracy Now, 10 de diciembre de 2010, https://www.youtube.com/watch?v=5CHdzxgy9rw

s/a, *Why the Pentagon Papers Still Matter Today*, Retro Report, The New York Times, 26 de marzo de 2017, www.nytimes.com/video/us/politics/100000005003643/lies-leaks-and-consequences.html?action=click&gtype=vhs&version=vhs-heading&module=vhs&region=title-area