Universidad Nacional Autónoma de México
Facultad de Estudios Superiores Aragón

Espionaje y filtraciones en el siglo XXI:

El caso WikiLeaks en Canadá

T E S I S

Que para obtener el título de
Licenciada en Relaciones Internacionales
P r e s e n t a:

Berenice Fernández Nieto

Asesora: Doctora Camelia Nicoleta Tigau

México, 2014

AGRADECIMIENTOS

A mi familia: Por estar siempre ahí, a mi padre, a mi madre, a mi padrino, Roberto Montoya, y a todos los que directa e indirectamente colaboraron a la realización de este proyecto. A mis compañeros de trabajo y a los amigos entrañables, en especial a Julio Cedillo Caballero, porque siempre me brindó su apoyo, guía y comprensión, a Norma Ventura, Maricruz, Axel, Ricardo, Vero, Grecia, Rosa, Karen y a todos aquellos que me enseñaron el valor real de la amistad.

"Menfis y Tebas quedan destruidas, Babilonia y Persépolis son incendiadas, Atenas y Roma se ven asediadas y saqueadas; desde el Norte al Este acuden ríos humanos de caballeros, hambrientos de trigo, de lujo y de sol, salvan los confines, cruzan los mares, someten y despojan a los antiguos señores ahora reblandecidos. Mientras tanto, los emperadores hacen asesinar y son asesinados, los nuevos reyes ordenan carnicerías a su turno concluyen siendo sacrificados. Y a pesar de todo, a pesar de esa sangre y ese odio, de esa ferocidad y esas traiciones, los hombres sobreviven y se renuevan". Giovanni Papini

A mis maestros, especialmente a la doctora Tigau por ser una excelente persona, a mis profesores: Arturo Ponce Urquiza, Víctor Monroy Olguín, Laura Navarrete, Sergio Verdejo, Cristina González, Erick Damián, Luis Manuel López, David García, Alva Valentina Canizal y Manuel Ferez. A la doctora Edit Antal Fodoroczy, Elizabeth Gutiérrez y a los investigadores del CISAN con los que tuve el gusto de trabajar. Por su ejemplo e impulso.

"No sé lo que pareceré a los ojos del mundo, pero a los míos es como si hubiese sido un muchacho que juega a la orilla del mar y se divierte de tanto en tanto encontrando un guijarro más pulido o una concha más hermosa, mientras el inmenso océano de la verdad se extendía, inexplorado frente a mí.". Isaac Newton

A la UNAM, al CISAN y a la Facultad de Estudios Superiores Aragón por el gran esfuerzo que día a día dedican para sembrar las semillas del futuro.

"El pájaro rompe el cascaron. El cascarón es el mundo. El que quiera nacer, tiene que romper un mundo"
Hermann Hesse

Y especialmente a mi abuela Amparo González y a mi tía Isabela Fernández, por todo lo que me enseñaron y porque siempre ocuparán un lugar en mi memoria. Por haber sido, como diría Dante, suspiros que hacen temblar el aire eterno.

ÍNDICE

Lista de Ilustraciones

Figuras

Gráficas

Mapas

Tablas

Introducción

El constante avance tecnológico transforma día a día el escenario sobre el que se llevan a cabo las relaciones diplomáticas. Aunado a ello, la forma en la que los Estados se relacionan y negocian depende en buena parte de los datos que sobre el otro agente se tenga, es aquí cuando surge el ciberespionaje como medio estratégico para obtener información privilegiada ya sea interceptando comunicaciones o por medio de la filtración de documentos confidenciales. Por esta razón, es necesario analizar el papel que las tecnologías de la información y la comunicación (TIC) y específicamente la Internet están tomado en el mundo de la diplomacia, prestando especial atención al caso del ciberespionaje y las filtraciones.

El uso cada vez más frecuente de las tecnologías de información y de las redes sociales colocan a las Relaciones Internacionales dentro de nuevos campos de interacción social e intercambio de datos, por lo que en la actualidad los Estados requieren tanto de herramientas jurídicas adecuadas para garantizar que el tránsito de información se dé dentro de un marco de legalidad, como de estrategias para evitar la fuga de información clasificada, todo ello en el marco de una nueva era en donde la innovación y el desarrollo tecnológico pueden ser factores tanto a favor como en contra de los Estados.

El caso *WikiLeaks* surge en este contexto promoviendo una reflexión en torno al potencial que las tecnologías poseen en el siglo XXI. En éste sentido el desarrollo de nuevas formas de interacción social ha alterado el número de actores en la escena internacional, ya que gracias al uso de las TIC han aparecido entidades como *WikiLeaks* y también se le ha otorgado mayor proyección a los organismos no gubernamentales y a las demás entidades internacionales ya existentes. Las repercusiones que el fenómeno *WikiLeaks* generó en diversos países, entre ellos Canadá, son de enorme importancia y a la vez le demuestran a la comunidad internacional la necesidad de una diplomacia pública efectiva y a la vanguardia tecnológica.

En la actualidad, las capacidades que otorga el uso de nuevas tecnologías son de enormes alcances y sin precedentes. Por un lado, su intervención puede ayudar a que se fortalezcan regímenes totalitarios, y por el otro pueden tener consecuencias en pro de la democracia, la libertad, los derechos humanos y la justicia.

El presente estudio analiza el surgimiento de una nueva amenaza para el sistema internacional: el ciberespionaje y la necesidad de incluirlo dentro de los análisis de seguridad nacional. De forma general el ciberespionaje consiste en un conjunto de actividades ilícitas que utilizan como herramienta principal las nuevas tecnologías y en especial Internet para interceptar, sustraer e incluso modificar información que por su naturaleza es considerada de carácter confidencial, perteneciente a determinados individuos, empresas, organizaciones o gobiernos.

Por lo anterior, la diplomacia contemporánea enfrenta un importante desafío puesto que las tecnologías evolucionan de forma continua y actualmente son utilizadas para la comunicación entre los Estados-nación. Por esta razón, es importante realizar un estudio sobre las consecuencias del fenómeno *WikiLeaks* en los ámbitos diplomático, político y social. Si bien existen importantes estudios al respecto, son pocos los que toman en cuenta su impacto en la diplomacia tradicional. También es preciso estudiar su efecto en el plano internacional y de forma particular lo que refiere a Canadá, puesto que sus publicaciones han logrado permear diversos sectores de la sociedad, políticamente es claro que generará cambios y es justo ahí donde radica la importancia de éste trabajo, ya que dicha organización mediática demuestra que las dimensiones del secretismo, espionaje, filtración, transparencia, participación social y la diplomacia no pueden ser las mismas en el siglo XXI.

El caso *WikiLeaks* es apreciado desde el plano internacional como un reto para la diplomacia y como una amenaza para la estabilidad mundial, pero también hay quienes lo ven como una buena alternativa en pro de la transparencia y a favor de la ciudadanía.

Cada día el número de participantes en el ciberespacio aumenta, por lo que es necesario reflexionar sobre las prácticas diplomáticas tradicionales y la nueva escena internacional. Sitios como *WikiLeaks* demandan mayor transparencia en los gobiernos y se pronuncian a favor de la libertad de información, por consecuencia los Estados tendrán que replantear la forma en la que se comunican con sus ciudadanos y dotar a los órganos gubernamentales de herramientas óptimas para una comunicación efectiva, y a la vez tendrán que implementar nuevas medidas para la protección de sus comunicaciones con el resto del mundo.

Por esta razón es preciso analizar las consecuencias que las filtraciones de *WikiLeaks* generaron en el ámbito diplomático, pues para Canadá como para el resto de los países involucrados, la publicación de documentos confidenciales significó un golpe importante en el manejo de sus relaciones diplomáticas; sin embargo, las reacciones tanto por parte del gobierno canadiense como por parte de la ciudadanía son diversas.

El propósito de analizar el caso canadiense surgió al descubrir que fue una de las primeras naciones en adoptar una agenda a favor de las TIC. Por ello apareció la necesidad de realizar un balance sobre los costos y beneficios que las nuevas tecnologías han generado en Canadá (tanto en la población como en la dinámica estatal), y en este contexto analizar los efectos del fenómeno *WikiLeaks* en la política interna y en la diplomacia canadiense.

El objetivo de la presente investigación es responder a las siguientes interrogantes: ¿Cuáles han sido los cambios en las Relaciones Internacionales que han permitido el ciberespionaje?, ¿A qué se debe el surgimiento de *WikiLeaks*? Y ¿Cómo afecta la práctica diplomática de países como Canadá?

Para lo cual se han establecido los siguientes propósitos:

- Analizar el desarrollo del espionaje a través la historia y examinar el surgimiento de los primeros problemas de ciberseguridad (específicamente de ciberespionaje) en el sistema internacional.

- Profundizar sobre uso de las nuevas tecnologías en el ámbito de las relaciones internacionales y en este contexto comprender las transformaciones que han generado tanto en la práctica diplomática como en los conflictos bélicos.

- Indagar los antecedentes, surgimiento, funcionamiento y objetivos de la organización *WikiLeaks* y evaluar su impacto tanto en la diplomática tradicional como en el periodismo, los movimientos sociales y en la estructuración de normas orientadas a la regulación de Internet.

- Examinar las publicaciones más importantes de *WikiLeaks* relacionadas con Canadá; evaluar su impacto en la sociedad, los medios de comunicación, la política nacional y en

la diplomacia, y determinar los retos que el gobierno canadiense enfrenta ocasionados por la incorporación de nuevas tecnologías en las dinámicas sociales y estatales.

El enfoque teórico bajo el que se desarrolla esta investigación es la Teoría de las Comunicaciones ya que consiste en una serie proposiciones que explican los aspectos políticos de las comunicaciones, así como el grado en que éstas condicionan el comportamiento y la evolución de la sociedad. Esta teoría resulta la más adecuada puesto que se encarga de la construcción de modelos, la aplicación de análisis cuantitativos y del análisis del papel de las comunicaciones en el campo de la realidad social en general y de la política internacional en particular, también considera al sistema político una red de comunicaciones en la que la información ocupa un lugar especial.

La hipótesis que sustenta este trabajo es que el avance tecnológico y la ausencia de medidas de seguridad adecuadas han permitido que el ciberespionaje y las filtraciones tengan mayores alcances. En este sentido *WikiLeaks* demuestra el potencial que las nuevas tecnologías pueden alcanzar en el siglo XXI y también representa a una sociedad cada vez más activa en el ámbito político e internacionalmente más conectada, lo que requerirá de nuevas medidas por parte de los Estados para poner en sincronía la práctica diplomática y las innovaciones tecnológicas. En especial Canadá deberá ampliar el espacio de interacción con la ciudadanía, mejorar los mecanismos de transparencia institucional e implementar nuevas medidas de seguridad cibernética.

La presente tesis se compone de cuatro capítulos. El primero (marco histórico) estudia antecedentes del espionaje a través de conflictos bélicos, por tal motivo se recorre su papel en diversas etapas históricas hasta llegar a la época actual. También se abordan Convenciones, así como otros instrumentos del Derecho Internacional que intentan combatir el ciberespionaje y los problemas de ciberseguridad. Asimismo, se toman en cuenta los recientes esfuerzos por parte de determinadas naciones, bloques regionales y organizaciones mundiales con el fin de promover la protección de las comunicaciones electrónicas.

El segundo capítulo (marco teórico) analiza la transformación del escenario internacional con el arribo de las nuevas comunicaciones y la evolución de la diplomacia, para dar paso al estudio de conceptos como diplomacia electrónica y ciberguerra. Posteriormente se abordan

las filtraciones y el espionaje electrónico en el ámbito diplomático y su significado en el marco de la Era tecnológica. En adición, se examina el papel de la Sociedad de la información y su relación con la nueva diplomacia, para dar paso al análisis del Estado, el poder y la revolución tecnológica. Por todo lo anterior, se adoptan diversas concepciones teóricas como las de *Karl W. Deutsch* que estudian los efectos que las comunicaciones producen en el comportamiento y en el desarrollo de la sociedad; *Celestino del Arenal* quien considera que el nivel de desarrollo de los medios de comunicación determina la configuración de la dinámica internacional; *Joseph Nye Jr.,* quien se ha especializado en los alcances de las TIC en la constitución y en el funcionamiento del Estado, y *Kenneth Hacker* y *Jon Van Dijk*, quienes proponen un modelo sistémico-dinámico de la estructura internacional caracterizado por la interacción de múltiples centros de poder, entre otras proposiciones.

El tercer capítulo analiza los efectos de *WikiLeaks* en la diplomacia, donde se examinan antecedentes, influencias, actividades y consecuencias; reacciones en el ámbito internacional, periodístico y social, entre otros factores, tomando en cuenta los retos que la organización (*WikiLeaks*) representa para el periodismo y la diplomacia tradicional. También se analiza la relación entre las nuevas tecnologías y los movimientos sociales así como las consecuencias políticas para Internet.

El cuarto y último capítulo versa sobre el caso *WikiLeaks* en Canadá. Por lo que se realiza un análisis general sobre las principales revelaciones, sus efectos en la esfera política, social y periodística canadiense para dar paso a una proyección sobre los retos que enfrenta Canadá en cuestiones como gobierno electrónico, transparencia institucional, participación social y reformas políticas orientadas a la regulación de Internet; finalmente se presentan las respectivas conclusiones. El presente trabajo parte de la filtración de cables diplomáticos realizados por *WikiLeaks* el 28 de noviembre de 2010 y se extiende al 28 febrero de 2014.

Esta investigación comenzó a elaborarse en la Facultad de Estudios Superiores Aragón en mayo de 2012 como parte de Servicio Social en el Centro de Investigaciones sobre América del Norte (CISAN). Se agradece especialmente al Proyecto PAPIIT IN301613, ¨Transformaciones recientes en la política y la economía de Canadá: una visión multidisciplinaria¨ por la beca que facilitó la realización del presente trabajo.

Capítulo 1. Historia del espionaje y problemas de ciberseguridad

En este capítulo se presenta una breve semblanza de actividades de espionaje registradas a lo largo de la historia, y se abordan los problemas de ciberseguridad que surgieron a la par de los avances tecnológicos de finales del siglo XX y principios del XXI.

1.1. Breve revisión histórica del espionaje

Dado que el ser humano es un ente social, inevitablemente debe comunicarse. A través del tiempo la comunicación ha constituido un elemento esencial tanto para el desarrollo de la civilización, como para la propagación del conocimiento; por esta razón, desde que el hombre emitió los primeros sonidos que dieron inicio al lenguaje hasta el establecimiento de vías de comunicación innovadoras y eficaces la información ha desempeñado un papel importante.

Antes que el hombre adoptara los primeros modelos de organización colectiva la comunicación ya ocupaba un lugar central, pues los medios de enlace los dieron paso a un nivel mayor de cohesión entre habitantes de un mismo espacio, colaborando a la construcción y conservación de tradiciones y costumbres.

Por lo anterior, resulta complicado determinar la fecha exacta en que surgieron las primeras prácticas de espionaje, al respecto hay quienes incluso se remontan al periodo neolítico.[1] Sin embargo, desde la presente perspectiva se puede señalar que el espionaje es una actividad endémica en la historia de las relaciones internacionales, y que aún en la actualidad representa una práctica estratégica en los procesos de interacción global.

A través del tiempo el avance en el conocimiento de las ciencias hizo posible el florecimiento de diversas civilizaciones; sin embargo, así como surgieron herramientas para conservar y propagar datos también aparecieron métodos para interceptar, manipular y sustraer información transcendente relacionada con los ámbitos social, económico, científico, etc. En los campos político y militar el manejo y la transferencia de información se convirtieron en recursos estratégicos para el porvenir de las naciones; recolectar y proveer datos clave funcionó como herramienta especial para la obtención de tierras o el dominio de

[1] Herrera Hermosillo, Juan Carlos. (2012). *Breve Historia del Espionaje*. Madrid: Nowtilus.

rutas comerciales y recursos naturales. Como consecuencia, la capacidad de acción de los Estados-nación se ha determinado por la efectividad de sus medios de comunicación. Desde siempre la información y las vías de conexión han determinado el nivel de desarrollo de las naciones, ocupan un lugar fundamental en la difusión del conocimiento y en la interacción social, económica y política de toda nación, de ahí que el célebre estratega militar Napoleón Bonaparte afirmara: "el secreto de la guerra está en las comunicaciones".[2]

Por lo tanto, para examinar la transformación de las prácticas de espionaje —y dado que la historia de la humanidad está ineludiblemente marcada por diversos enfrentamientos— se analizará su evolución durante los periodos de guerra.

Desde el establecimiento de las primeras ciudades el hombre se ha servido de todos los medios disponibles para mantenerse siempre informado. A través del tiempo reyes, emperadores, zares y demás mandatarios, han otorgado un lugar especial a los servicios de recolección de datos. Esta necesidad por mantenerse al tanto de lo que acontece en otros territorios —entorno social, político, económico y militar— hizo posible que el espionaje no sólo fuera aceptado, sino perfeccionado. Ya sea en tiempos de paz o de guerra el mantenimiento de fuentes confiables de información logró proveer datos estratégicos a los dirigentes de distintas naciones; contar con reportes relacionados con enfrentamientos, concertaciones, conflictos sociales, acuerdos comerciales, etc. logró marcar una gran diferencia en desenlace de cientos de batallas.

1.1.1. Antigüedad (4000 a. C. – 476 d. C.)

Aunque la mayor parte de los estudios sobre la historia del espionaje se remontan al periodo que antecede la Primera Guerra Mundial existen trabajos como el de Juan Carlos Hermosillo Herrera (2012) que van más allá, situando su origen en el periodo neolítico durante los enfrentamientos de *Thalheim* (en Alemania) hace aproximadamente 7500 años;[3] las ruinas sugieren que se suscitó un enfrentamiento entre dos grandes tribus, y que uno de los

[2] Glassford, Lieut. W. A. (Octubre 30, 2002). "The Signal Corps".*US Army Center of Military History*. [En línea]. Disponible en: <http://www.history.army.mil/books/R&H/R&H-SC.htm>. (Consulta 09/05/2014).
[3] Schulting, Rick J. y Linda Fibiger. (Edit.). (2012). *Sticks, Stones, and Broken Bones: Neolithic Violence in a European Perspective*. Oxford: Oxford.

contrincantes obtuvo información estratégica sobre la población que atacó, lo que sin lugar a dudas le otorgó una ventaja importante en el desarrollo y desenlace del conflicto.

Poco a poco, las tareas de espionaje fueron abarcando distintos aspectos, según Hermosillo Herrera antes de conquistar los pueblos sumerios (entre 2300 y 2700 a. C.) Sargón I "el grande" envió vigilantes a territorio enemigo con el objetivo de recolectar información geográfica de la zona, gracias a ello obtuvo datos que le permitieron dominar gran parte de Mesopotamia. Otra huella importante sobre actividades de espionaje durante la Antigüedad son las tablillas escritas en acadio que datan de entre 1800 y 1750 a. C. y que fueron elaboradas poco antes de que Hammurabi, sexto rey de Babilonia, destruyera la ciudad Mari (en Siria), en ellas se hace referencia por primera vez al proceso de recolección de datos. Según las tablillas, el rey de Mari (Zamri- Lim) logró infiltrar agentes a la corte del rey Hammurabi, estos colaboradores formaron los primeros espías diplomáticos de los que se tenga registro. Por lo que, con el paso del tiempo, la recolección de datos se convirtió en un proceso esencial para la protección y el bienestar de las naciones.

A través de la historia los servicios de información han jugado un papel decisivo en el desenlace de numerosas batallas, por ello en el ámbito militar el espionaje se convirtió en una especialidad. Al respecto, la obra *El arte de la Guerra* (escrita por Tzu Sun Tzu aproximadamente en el año 500 a. C.)[4] señala que es muy importante conservar fuentes que compartan información sobre la condición del enemigo, ya que según Sun Tzu de ello depende la victoria y la gloria de una nación. También hace especial énfasis en el uso de espías, de los que incluso elabora una clasificación.[5]

Avanzando unos en la historia, durante la segunda mitad del siglo IV a.C. Alejandro III de Macedonia también recurrió al uso de espías para derrotar a sus enemigos. Antes de iniciar la batalla de Gaugamela (75 millas al oeste de Arbela), en el año 331 a.C.,[6] Alejandro III a través de lo que Tzu Sun Tzu identificaría como "espías liquidables" hizo creer al

---

[4] Hernández Gómez, José Ricardo. "Sun Tzu. El arte de la Guerra". *Revista virtual de inteligencia.* [En línea]. Disponible en: <http://revistadeinteligencia.es.tl/Sun-Tzu-d--Cap%EDtulo-XIII.htm>. (Consulta 16/07/2013).

[5] Espías nativos.- pertenecen al lugar del que informan; espías internos.- que forman parte del gobierno enemigo; agentes dobles.- contratados entre espías del adversario; espías liquidables.- los que otorgan información falsa al enemigo; espías flotantes.- que retornan para presentar el resultado de sus investigaciones. Fuente: Sun Tzu. (2005). *El arte de la guerra.* México: Leyenda.

[6] Hermosillo Herrera. *Óp. Cit.*

enemigo, Darío III, que la batalla comenzaría por la noche. La ofensiva inició hasta la mañana del día siguiente, cuando el ejército de Darío estaba debilitado por haber esperado inútilmente el ataque. Como consecuencia, gracias al uso de espías y a las grandes tácticas militares utilizadas por Alejandro el ejército macedonio obtuvo la victoria sin importar que las tropas de Darío fueran más numerosas.[7] Desde entonces el uso del espionaje en el ámbito militar se convirtió en un arma especial, y al mismo tiempo los Estados comenzaron a establecer vías de comunicación confidenciales, adoptando el uso de códigos especiales con el fin de proteger el intercambio de información oficial dentro y fuera del territorio. Sin embargo, para cada nuevo mecanismo surgió una contraparte, los métodos de intercepción, robo, manipulación y decodificación también evolucionaron, dando inicio a una especie de competencia en el desarrollo de tecnologías para el intercambio y resguardo de datos.

1.1.2. Edad Media (476 d.C. - 1453)

Es necesario señalar que la palabra "espía" fue utilizada por primera vez en el medioevo, en ese entonces se usó para describir a agentes alemanes que actuaban en territorio italiano. En 1264, el escritor Tomaso Garzoni los describió como: "[…] una clase de personas que secretamente entran en una ciudad para referir a su propio ejército información acerca del enemigo".[8] También durante este periodo el uso de espías diplomáticos se propagó de forma importante por toda Europa. A principios del siglo XV el ambiente de incertidumbre ante las verdaderas funciones de un representante era tal, que el Rey Enrique V de Inglaterra ordenó encarcelar a todos los representantes franceses mientras elaboraba un plan para invadir ese país, de esta forma eliminó el temor de que los embajadores pudieran obtener información secreta sobre los planes del reino.

Continuando con la revisión, durante el siglo XIII las tácticas de espionaje y los sofisticados sistemas de comunicación militar desarrollados por el ejército, permitieron que el imperio

---

[7] Caballero Díez, Juan Andrés. (Noviembre, 2011). "Gaugamela e Hidaspo dos grandes victorias de Alejandro Magno". *Mundo Historia*. [En línea]. Disponible en: <http://www.mundohistoria.org/blog/articulos_web/labatallahidaspo-326-ac-la-ultima-batalla-alejandro-magno>. (Consulta 23/08/13).

[8] Juárez Valero, Eduardo. (Diciembre, 2012). "Espías y agentes dobles durante la Edad Media". *Historia National Geographic*, No. 109. [En línea]. Disponible en: <http://www.nationalgeographic.com.es/articulo/historia/secciones/7942/espias_agentes_dobles_durante_edad_media.html>. (Consulta 25/08/13).

mongol resultara victorioso en numerosas campañas militares.[9] De acuerdo con Jonathan King (2009) debido a que Gengis Kan (líder del imperio) consideraba esencial poseer información sobre los territorios a conquistar, los mongoles lograron desarrollar excelentes sistemas de comunicación e inteligencia. La recolección de datos fue tan importante que era imposible comenzar una invasión sin haber recabado información sobre diversos aspectos del territorio enemigo. Entre los alcances más sobresalientes de este imperio están: la conquista del continente asiático bajo el mandato de un solo líder y la creación de un sistema de comunicación capaz de transmitir información entre Mongolia y Europa. En este último aspecto destaca el uso del *yam*, el cual consistía en un servicio de correos encargado de reunir y distribuir reportes de inteligencia a lo largo de todo el imperio. Gracias a este sistema Gengis Kan logró someter por completo al continente asiático, pues la red poseía cientos de caballos y de mensajeros listos para transportar información a través del enorme territorio,[10] los mensajeros también actuaban como espías o agentes secretos, encargados de obtener información relevante sobre las áreas que visitaban durante sus largos trayectos, mientras que las estaciones *yam* se encargaban de vigilar a los viajeros. De acuerdo con Jonathan King (2009), este sistema es considerado uno de los logros más grandes del imperio mongol, ya que su fama se extendió por todo el continente y su prestigio se conservó aun después de la caída del imperio a manos del ejército otomano.

Por otra parte, hacia finales del siglo XV el establecimiento de representaciones oficiales permanentes significó una enorme ventaja para los servicios de información del Estado, pues representaron una fuente de comunicación estable.[11] Al respecto, en una relación de la embajada de Roma escrita en el siglo XVII se establece:

> *La segunda cosa que toca al ofizio* [sic] *de embajador es ser una espía calificada, que no sólo atienda a descubrir las acziones* [sic] *y motivo desteprizipe* [sic], *sino también sino de todos los demás de Ytalia* [sic] *y fuera de ella por la notizia* [sic] *que aquí puede hazer* [sic] *por medio de sus ministros y*

[9] King, Jonathan. (2009). "Intelligence Gathering of the Mongolian Empire". *Études Historiques*, Vol. 1, No. 2. [En línea]. Disponible en: <http://www.etudeshistoriques.org/index.php/etudeshistorique/article/viewFile/7/7>. (Consulta 23/08/13).

[10] De acuerdo con Jonathan King, Francis Dvornik hace referencia a la inteligencia del imperio Mongol empleada durante un ataque a China, gracias a la cual lograron encontrar un punto débil en la "gran muralla". En: *Origins of Intelligence* Services. (1974). New Brunswick: Rutgers University Press.

[11] Calduch Cevera, Rafael. (1993). *Dinámica de la Sociedad Internacional*. Madrid: CEURA.

otras inteligencias y para conseguir esto es menester poner gran cuidado en elegir los medios que son a propósito y más eficazes [sic].[12]

Con esto es posible observar que entre las principales funciones de un representante diplomático está subministrar información sobre las condiciones políticas, sociales, económicas, etc. del país anfitrión. Sin embargo, no significa que la función del representante oficial y la del espía sean las mismas, la diferencia recae en los métodos para recabar información; pues mientras el agente diplomático puede rendir un informe detallado sobre aquellos asuntos que su condición oficial le ha permitido conocer, para el espía el objetivo primordial es obtener la mayor cantidad de datos sobre el asunto que le ha sido asignado valiéndose de toda clase de métodos, algunos de los cuales a menudo caen en la ilegalidad.

Durante la Edad Media las actividades de espionaje se orientaron a la protección y la conservación de territorios, en esta época el desarrollo de las prácticas de espionaje fue limitado. Si bien los enfrentamientos en dicho periodo provocaron la transformación de las técnicas de recolección de datos, la subsecuente revolución científica que logró influir en los modelos de producción, los transportes y hasta en el pensamiento político de la edad moderna le daría un impulso mayor.

1.1.3. Edad Moderna (1453-1789)

Durante este periodo se suscitó un impresionante desarrollo en el campo de las ciencias, los avances generados en diversas disciplinas transformaron la forma de vida de miles de personas. La evolución de las comunicaciones permitió el intercambio de información a través de nuevos medios y rutas. A lo largo de esta época el descubrimiento de nuevas tierras, las transformaciones ideológicas y sociales en Europa, la conquista de África y los avances científicos y tecnológicos permitieron que el espionaje encontrara nuevas áreas de aplicación.

En la era moderna es posible encontrar un ejemplo del uso del espionaje durante la conquista española al continente americano en la batalla de Tucapel (en 1553). A principios del siglo XVI el conquistador Pedro Valdivia estableció varios asentamientos a lo largo del río Maule,

[12] Navarro Bonilla, Diego. (2005). "Información, Espionaje e Inteligencia en la Monarquía hispánica (Siglos XVI-XVII)". *Revista de historia militar*, pp. 13-34. [En línea]. Disponible en: <http://www.portalcultura.mde.es/Galerias/revistas/ficheros/RHM_serviciosinformacionmodernos.pdf>. (Consulta 11/08/2013).

territorio mapuche (en Chile), poco después se sumó a su servicio un nativo llamado Lautaro; sin embargo, las verdaderas intenciones del joven mapuche estaban completamente alejadas del servicio a los conquistadores, ya que, poco a poco, se dedicó a aprender el uso de las armas españolas, montar a caballo e incluso organizó un sistema de espías y mensajeros, esperando el momento preciso para liberar a su pueblo. Una noche de diciembre de 1553[13] Lautaro animó a la población a luchar en contra de los españoles, como resultado del enfrentamiento Pedro Valdivia fue asesinado y el resto de sus colaboradores expulsados del fuerte de Tucapel.

Empero, esta táctica no tuvo el mismo éxito en el caso de Hernán Cortés. El conquistador había advertido a los tlaxcaltecas las consecuencias de alguna traición de su parte. No obstante, los gobernantes de Tlaxcala decidieron enviar a un grupo de nativos para vigilarlo. Cortés descubrió a los espías, quienes confesaron que los Tlaxcaltecas planeaban atacar esa noche. Como advertencia Hernán Cortés ordenó mutilar sus manos y enviarlos de vuelta a Tlaxcala para mostrar lo que le sucedería a quienes intentaran espiarlo de nuevo.[14]

En esta época el espionaje se orientó a recabar información geográfica de los nuevos territorios en busca de la expansión de dominios europeos en el continente americano, también adquirió importancia el espionaje militar, pues a menudo los informes se concentraban en el número de elementos con los que contaban las potencias europeas en la zona, y en la cantidad y tipo de armas que poseían.

En el siglo XVIII durante la guerra de independencia estadounidense, George Washington creó un pequeño grupo de espías conocido como *The Culper Ring* que se mantuvo activo durante el transcurso del conflicto. A principios de 1775 no existía ningún oficial u oficina de inteligencia en la facción patriota, y dadas las circunstancias era urgente conformar un organismo que contara con espías calificados, por lo que a mediados del año siguiente Washington propuso estructurar una red de espías que operara exclusivamente en Nueva York, ya que representaba un bastión importante para Gran Bretaña. En un principio enviaron agentes inexpertos que en la mayoría de los casos terminaban capturados por

[13] Guzmán, Jorge. (1993). *Ay mamá Inés: crónica testimonial*. Santiago de Chile: Andrés Bello.

[14] Espino López, Antonio. (Julio-diciembre, 2012). "Granada, Canarias, América: el uso de prácticas aterrorizantes en la praxis de tres conquistas, 1482-1557". *Historia*, No. 45, Vol. II, pp. 369-398. [En línea]. Disponible en: <http:// www.scielo.cl/pdf/historia/v45n2/art01.pdf>. (Consulta 11/08/13).

autoridades británicas o eran reclutados como agentes dobles. Como consecuencia en 1778 Benjamin Tallmadge propuso a Washington establecer agentes permanentes en el círculo conservador con el objetivo de inspirar confianza, haciéndose pasar como miembros leales y de de esta forma obtener información valiosa. El grupo de espías tuvo gran éxito, pues lograron establecer conexiones cercanas con oficiales británicos, gracias a ello se obtuvo información militar clave para que George Washington alcanzara la victoria. *The Culper Ring* adquirió rápidamente nuevas habilidades de espionaje y sentó las bases de los servicios de inteligencia modernos.[15]

En lo que respecta al continente europeo, los líderes de grandes imperios ya habían comprendido el valor estratégico del espionaje. Durante el siglo XVII el ejército francés contaba con dos importantes subdivisiones: una encargada de recolectar información sobre el enemigo y la otra, dedicada a recabar datos sobre asuntos particulares del general Bonaparte.[16] En relación al espionaje Napoleón Bonaparte consideraba que: "un espía en un lugar adecuado vale tanto como veinte mil soldados en el campo de batalla". Para Napoleón, Karl Schulmeister era ese elemento importante, pues colaboró en buena medida a las victorias del emperador, prestando servicios como agente doble. En 1805 Shulmeister se embarcó a Viena con el objetivo de infiltrase en el ejército austriaco, para ello afirmó que había sido expulsado de Hungría por cargos de espionaje en contra de Napoleón. De esta forma logró convencer al comandante Mack de que lucharía contra Francia. Poco después consiguió que le nombraran jefe de los Servicios de Inteligencia. A finales de ese mismo año, la alianza conformada por Gran Bretaña, Austria, Rusia y Suecia estructuró un plan para terminar con el creciente poder de Napoleón en el continente, por esta razón lanzó un ataque por tierra y mar en contra de las fuerzas francesas. Sin embargo, el comandante Mack avanzó sin esperar al ejército ruso y continuó su rumbo hacia Viena siguiendo los consejos de su recién nombrado jefe de Servicios de Inteligencia. Al llegar al Ulm, Mack y el ejército austriaco fueron rodeados por las fuerzas

[15] Armchair General. (Marzo, 2009). "The Culper Ring". *Arose.squarespace*, Vol. IV, No. 1, pp. 26 -27. [En línea]. Disponible en: <http://arose.squarespace.com/storage/articles/Culper_Rin g.pdf>. (Consulta 25/08/13).

[16] Barrera Orellana, Felipe. (2009). *Análisis de la actividad de inteligencia del Estado y su control público jurídico.* (Tesis de Licenciatura). Universidad de Chile, Facultad de Derecho, Santiago de Chile. [En línea]. Disponible en: <http://tesis.uchile.cl/bitstream/handle/2250/106894/de-barrera_f.pdf?sequence=3>. (Consulta 30/08/13).

de Napoleón. Poco después, el 20 de octubre de 1805, el comandante Mack fue oficialmente derrotado.[17]

En resumen, durante la Edad moderna el espionaje fue refinando sus actividades, especializándose en distintas áreas particularmente en el campo militar, impulsado por los avances científicos que caracterizaron la época. En este periodo el espionaje experimentó una importante evolución, pues no sólo fue adoptado en el transcurso de conflictos militares, sino que, poco a poco, surgió la necesidad de preparar agencias de inteligencia que funcionaran también en tiempos de paz.

1.1.4. Época Contemporánea (1789- la actualidad)

Con la Revolución francesa se marca el fin de una era en la historia de las relaciones internacionales, dando paso a una etapa caracterizada por el surgimiento de dos grandes conflictos. Por primera vez en la historia el hombre conoció los alcances de las batallas mundiales, en las que se desarrollaron una serie y tipos de armamentos como nunca antes se hubiera imaginado. Los periodos de guerra legaron a la humanidad lamentables episodios de hambre, miseria, genocidios y enfermedad cuyos efectos lograron marcar a más de una generación. Entre tanto, los métodos para preservar la seguridad nacional, regional y mundial se modernizaron. En este contexto el espionaje lejos de quedar en el olvido cobró fuerza día a día. Desde estallido de la Gran Guerra hasta la actualidad las comunicaciones han reafirmado su importancia en la arena internacional. Aunado a ello, hacia finales del siglo XX y principios del XXI se ha experimentado una importante evolución en las comunicaciones. Con la llamada Revolución tecnológica se abrió camino a la Sociedad del conocimiento en la que tanto líderes nacionales como figuras políticas, centros de pensamiento, comités nacionales e internacionales, círculos de expertos y hasta un simple individuo tienen a su alcance una enorme cantidad de datos. En adición el surgimiento de nuevo espacio, donde establecer límites jurisdiccionales resulta complicado, coloca a los Estados y a los organismos de seguridad en un terreno complejo y en donde conceptos como "espionaje", "sabotaje" y "sustracción ilícita" no han perdido validez.

[17] Milecki, Andrzej. "Schulmeister Karl Ludwig (1770 - 1853)". *Napoleon.org.pl.* [En línea]. Disponible en: <http:// www.napoleon.org.pl/polityka/schul.php>. (Consulta 30/08/13).

Sin duda alguna el siglo XX será recordado por los enfrentamientos suscitados entre diversos Estados-nación, en los cuales la tecnología militar alcanzó límites insospechados. Por lo anterior, es necesario analizar *grosso modo* que ocurrió con el espionaje durante este periodo, para posteriormente examinar las consecuencias del avance tecnológico en el ámbito de la seguridad.

Retomando al continente americano, de acuerdo con Mark C. Hageman (*s.f.*) durante la Guerra de Secesión (1861-1865) en el ejército confederado operaba una red de espionaje creada por Thomas Jordan a finales de 1860, aunque en ninguna de las partes (los confederados y los miembros de la Unión) existía de manera oficial un organismo especializado, ambas facciones intentaron estructurar entidades de inteligencia y espionaje. Según Hageman la improvisada red de espías logró proveer al sur de importantes datos relacionados con el ejército enemigo. Progresivamente, los Confederados lograron formar nuevos grupos de espías, de entre los cuales destacan Thomas N. Conrad y Franklin Stringfellow. Tanto Conrad como Stringfellow participaron en la creación del primer organismo oficial de servicio secreto de la Confederación, y que formó parte de la oficina de señales de CSA (por sus siglas en inglés *Confederate States of America*).[18] El encargado de coordinar las actividades de espionaje y contraespionaje fue el mayor William Norris, los agentes a su cargo trabajaban en la llamada "línea secreta" la cual consistía en un pasaje subterráneo entre Richmond y Washington. Hageman también señala que Canadá se convirtió en un bastión importante de espionaje para los Confederados, y que por esa razón las operaciones se extendieron a la parte norte del territorio. Durante el conflicto el ejército Confederado también se sirvió de agentes privados que actuaron como espías y como medios para intercambiar comunicaciones confidenciales.

Por parte de los miembros de la Unión, el primer organismo de espionaje fue creado a mediados de 1861 por Allan Pinkerton, quien logró infiltrarse entre miembros de la Confederación.[19] La organización obtuvo información sobre los planes de ataque de la facción rival, mientras que Pinkerton consiguió disolver una importante red de espías del sur. Sin embargo, dada la inexperiencia de la red, en ocasiones los informes enviados al norte contenían datos imprecisos sobre el ejército enemigo. Fue a lo largo de este conflicto que apareció la

[18] Hageman, Mark C. "Espionage in the Civil War". *Spies, scouts and raiders*. [En línea]. Disponible en: <http://www. civilwarsignals.org/pages/spy/spy.html>. (Consulta 30/08/13).
[19] *Ídem.*

figura de Timothy Webster, el primer agente doble en la historia estadounidense. Según Hageman, Webster formaba parte del servicio de espionaje de la Unión pero simpatizaba las ideas de los Confederados, por lo que de forma secreta prestó sus servicios a dicha finalmente Webster fue descubierto y ejecutado por miembros de la Unión en Richmond. Por parte del ejército del norte destacan figuras como Elizabeth Van Lew, quien encabezó una de las más grandes y exitosas redes de espionaje en la historia; el general Lafayette C. Baker, recordado por la crueldad de sus métodos; Sarah Emma Edmonds, quien logró ingresar al sur gracias a un disfraz de esclavo, y el comandante Henry Young, quien ayudado por 58 colaboradores logró intervenir las líneas de telégrafo y las vías ferroviarias del enemigo.[20]

En síntesis, no fue sino hasta después de los enfrentamientos suscitados entre diversas naciones —principalmente ocasionados por expansión territorial y la emancipación de colonias europeas en América— que se lograron estructurar los primeros organismos de inteligencia en distintos países (véase tabla 1). Dichas entidades buscaban subministrar datos que pudieran ser útiles en caso de futuros enfrentamientos con antiguos enemigos, e incluso para identificar amenazas potenciales. Los informes relacionados con la constitución geográfica, desarrollo militar, composición social, prácticas mercantiles y demás actividades de distintos países, cobraron gran importancia e impulsaron la creación de agencias especializadas en su análisis las cuales fueron puestas a prueba con estallido de la Primera Guerra Mundial, pues a lo largo del conflicto los Estados lograron conocer las fortalezas y debilidades de su sistema, y las de los otros.

Tabla 1. Desarrollo de los primeros organismos de inteligencia, por países.

Alemania	1866	Se fundó una especie de ministerio exterior encargado de asuntos policiales y políticos que poco después fue nombrado "Policía del Servicio Secreto" encabezada por Wilheim Stieber. Posteriormente dicha división sería conocida como la Agencia Central de Inteligencia y logró establecer agentes en París, Londres y Viena. Los enormes alcances de la red espionaje alemán se debieron en gran parte a los esfuerzos de Stieber, pues consideraba que un sistema de espionaje masivo proveería una imagen íntegra de los enemigos de Alemania y de sus potenciales amenazas en Europa. Progresivamente los recursos destinados a dicha entidad aumentaron, por lo que llegó a ser la agencia de inteligencia mejor financiada en Europa (exceptuando a Rusia). Hacia finales del siglo XIX Alemania contaba con la mejor red de espionaje en toda Europa. En 1901 contaba

[20] *Ídem.*

		con 124 agentes distribuidos en Bélgica, Suiza, Inglaterra, Italia, España, Luxemburgo, Dinamarca, Suecia y Rumania.
Francia	1871	Después de la guerra con Prusia (1870-1871) se estableció la sección de Reconocimiento Militar y Estadística con el fin de obtener datos sobre alguna posible invasión por parte de tropas alemanas; posteriormente el organismo fue conocido como Servicio Especial y hacia 1880 contaba con agentes en Berlín, Dresde, Leipzig, Frankfurt, Colonia y Mannheim.
Reino Unido	1882	Se creó el Comité Exterior de Inteligencia que se encargaba de recibir reportes de la Real Armada Naval sobre las actividades de barcos extranjeros y de navíos mercantes en altamar, también reportaba los avances militares que podían observarse desde Berlín, Viena y San Petersburgo a través de agregados militares.
Estados Unidos	1822	Se crea la Oficina de Inteligencia Naval con el objetivo de recabar toda información que pudiera ser útil al Estado. En contraste con Europa Estados Unidos no contaba con una extensa red de espionaje, y al igual que Reino Unido los primeros organismos de inteligencia fueron establecidos por el Ejército y la Marina. Cuando en 1885 el Secretario de Guerra William C. Endicott solicitó información sobre las fuerzas armadas de un Estado europeo al general R. C. Drum quedó sorprendido al percatar que Drum no contaba con ningún dato, y tampoco poseía medios que le permitieran desempeñar dicha función. En consecuencia se creó la División de Información Militar, MID (por sus siglas en inglés) encargada de recopilar información militar que se pondría a disposición del Departamento de Defensa y del Ejército en general. Con el paso del tiempo se incorporaron más agentes que operaron principalmente Berlín, Paris, Roma, Viena y San Petersburgo.
Rusia	1900	Se funda el Departamento Especial conocido como *Okhrana* que se convertiría en el antecesor de una serie de organizaciones policiales secretas. Diversas dependencias monitorearon a los oponentes del Zar tanto dentro como fuera del territorio. Las agencias dedicadas al exterior operaron de forma especial en Francia, Suiza y Gran Bretaña (donde se reunían los disidentes del régimen zarista). Por su parte el cuartel general militar se encargaba, a través de diversas subsecciones, de estudiar las fuerzas militares de Alemania, Turquía, Persia, el imperio Astro-Húngaro, los Estados de la península de los Balcanes, y la región escandinava.

Fuente: Elaboración propia con datos de Richelson, Jeffery T. (1995). A Century of Spies Intelligence in the Twentieth Century. Nueva York: Oxford University Press.

Continuando con la revisión, con la llegada del siglo XX el campo de las Relaciones Internacionales sufrió grandes cambios. Los Estados-nación avanzaron hacia un periodo caracterizado por el desafío a las formas de convivencia mundial, a la solución pacífica de controversias y a los mecanismos cooperación entre naciones. La sociedad internacional enfrentó múltiples periodos de crisis reflejados en terribles episodios de guerra, específicamente en dos conflictos que fueron capaces de involucrar a gran parte del mundo y que más allá de representar un reto para la diplomacia y la preservación del sistema internacional, marcaron a la humanidad con niveles inesperados de pobreza y muerte. En este

contexto el desarrollo y especialización de prácticas militares dotaron a los servicios de inteligencia y al espionaje de una importancia central.

En junio de 1914 el asesinato del Archiduque Francisco Fernando en Serbia dio inicio al primer gran enfrentamiento de la época contemporánea. El 27 de julio de 1914 Austria, respaldada por Alemania, invadió Serbia quien a su vez recibió apoyo de Rusia y Francia. El 31 de julio de ese mismo año las tropas rusas comenzaron a movilizarse a través de la frontera germana, los puestos de vigilancia alemanes reportaron el movimiento y prepararon sus fuerzas. Poco después Prusia declara la guerra a Rusia e invade Bélgica,[21] con ello un ambiente de tensión se desató en Europa, pues las grandes potencias habían ingresado al campo de batalla. Las rivalidades causadas por el reparto de África durante la Conferencia de Berlín (1884-1885) habían jugado un papel fundamental para el estallido del conflicto, pues Francia y Gran Bretaña se unieron para contrarrestar el creciente poderío territorial germano, quien a su vez brindó apoyo al impero Austro-Húngaro.[22]

Las uniones formadas, de un lado, por Gran Bretaña, Francia y Rusia (la Triple Alianza) y del otro, por Prusia, el imperio Austro-Húngaro e Italia (la Triple Entente), esperaban el momento preciso para movilizar a sus agentes de inteligencia a territorio enemigo. Llegado el momento, el imperio Austro-Húngaro ordenó aumentar la vigilancia de Rusia y Francia, por lo que envió oficiales encubiertos bajo la identidad de inversionistas o turistas, que lograron remitir información codificada a través de telegramas y cartas, estos agentes consiguieron identificar un inusual intercambio de mensajes entre Rusia y Francia. Por su parte, Prusia contaba un representante en la corte del Zar que logró compartir información sobre el comportamiento de las tropas rusas que se dirigían a San Petersburgo. Por lo que durante el inicio del conflicto las actividades de inteligencia se concentraron en las áreas fronterizas de los Estados rivales. En ambas partes (La Triple Alianza y la Triple Entente), existieron espías que hicieron importantes colaboraciones para sus respectivos países. Particularmente del lado francés las actividades de espionaje se centraron en Bélgica, Holanda y las zonas galas bajo control germano, uno de los grandes logros del servicio de inteligencia francés fue infiltrar un espía en territorio germano que durante todo el

[21] *Ídem.*

[22] Adonon Djogbènou, Fabien. (2003). *Estudios Africanos*, Vol. II. México: UNAM. [En línea]. Disponible en: <http: //ciid.politicas.unam.mx/estudios_africanosII/EstudiosAfricanosII.pdf>. (Consulta 30/08/13).

enfrentamiento monitoreó cada movimiento de las tropas e incluso advirtió sobre el ataque a Verdun (al nordeste de Francia).[23]

Si bien los mecanismos de vigilancia conservaron la misma importancia que durante los enfrentamientos anteriores, no fue sino hasta la Primera Guerra Mundial que la tecnología ocupó un papel relevante, pues en este periodo se suscitaron grandes avances en las técnicas de recolección de datos como el surgimiento de nuevas herramientas de reconocimiento territorial, innovaciones en cuestión de aeronáutica y en equipos fotográficos. La aparición de estos instrumentos tuvo una enorme influencia en el transcurso de enfrentamientos como en las batallas del Marne, Somme, Tannenberg así como en diversos conflictos diplomáticos. Por lo tanto, la intercepción de comunicaciones militares y diplomáticas vía radio aumentó de forma considerable durante la Gran Guerra.

Después de la Primera Guerra Mundial las actividades de espionaje continuaron desarrollándose, aunque en menor medida debido a las consecuencias del enfrentamiento. De momento los deseos de expansión territorial en Europa se detuvieron, pues los efectos políticos, sociales y económicos de la guerra sacudieron a todo el continente. Mientras tanto Estados Unidos surgió como un fuerte país industrial y se colocó en el centro del sistema capitalista. La reducción presupuestal en las estructuras gubernamentales, producto de los costos de la guerra, afectó a las organizaciones de inteligencia en Europa y América. No obstante, en el caso de Alemania las restricciones militares impuestas y el endeudamiento interno derivados del conflicto provocaron que las principales técnicas de defensa se centraran en el campo de la inteligencia. Respecto a las otras naciones el resto de los organismos de inteligencia continuaron operando, ya que habían demostrado su utilidad a lo largo del enfrentamiento. Gran Bretaña creó en 1919 una academia especializada en códigos y cifrados que dependía directamente del Estado y durante las dos décadas siguientes la institución pasó del análisis de códigos militares al de códigos diplomáticos. El éxito de esta academia se refleja en los acuerdos alcanzados en la Conferencia de Lausana (1922-1923) —con el que se puso fin a los conflictos entre Turquía y Gran Bretaña y se establecieron las fronteras del Estado turco

[23] Richelson. *Óp. Cit.*

moderno—, pues Gran Bretaña logró interceptar telegramas turcos, obteniendo ventaja en la negociación.[24]

Durante la posguerra Estados Unidos transformó la oficina militar de cifrado en una organización militar, con la que logró interceptar múltiples comunicaciones entre ellas las de México con Alemania. La nueva organización se enfocó en descifrar comunicaciones europeas como las de Austria, Bélgica, Dinamarca, Finlandia, Grecia, Italia, Países Bajos, Noruega, Polonia, Portugal, Rumania, Suecia y Suiza. [25]

De acuerdo con Jeffrey Talbot Richelson (1995) tras la Primera Guerra Mundial los servicios de Inteligencia de Japón y Alemania se esforzaron por cubrir las demandas de una política exterior agresiva. Mientras que Estados Unidos, Gran Bretaña y Francia expandieron sus actividades como respuesta al creciente clima de tensión internacional, al tiempo en que los objetivos de espionaje por parte de la URSS aumentaban. Es posible definir a este periodo como la "época de expansión de los servicios de inteligencia" y particularmente del espionaje.

Las crisis políticas, sociales y en especial las económicas, le habían mostrado a las grandes potencias todo lo que había por perder en caso de una derrota. Por lo que, hacia el inicio de la Segunda Guerra Mundial las naciones privilegiaron los servicios de inteligencia, extendiendo sus actividades por diversos continentes.

En 1933 Adolf Hitler fue electo para la cancillería alemana, las acciones hacia un reposicionamiento alemán fueron evidentes, pues ordenó incrementar las actividades de inteligencia y solicitó nuevas operaciones de espionaje y contraespionaje militar. El 16 de marzo de 1935 Hitler restableció la conscripción militar, ignorando lo estipulado en el Tratado de Versalles y anunció el restablecimiento y aumento del ejército alemán. Al mismo tiempo las agencias de inteligencia se encargaron de investigar si se estaba planeando alguna respuesta militar por parte de Gran Bretaña, Francia, Italia, o alguna otra nación. Los alcances de los servicios de inteligencia nazi fueron tan importantes que lograron descubrir los planes de un encuentro en Stresa (Italia) programado para el 11 de abril de ese mismo

[24] *Ídem.*
[25] *Ídem.*

año. Dada la eficiencia de estos servicios el gobierno Alemán creó una Oficina de Investigación conformada por 20 colaboradores entre especialistas en señales de radio, técnicos, criptoanalistas, etc. que junto a otras organizaciones mantuvieron una extensa red de escuchas.[26]

El descontento alemán por las resoluciones del Tratado de Versalles sumado a los reclamos italianos respecto a la región costera de Dalmacia impulsaron el estallido de una nueva guerra. Aunado a ello los choques ideológicos en Europa ayudaron a encender el conflicto, ya que después de la Primera Guerra Mundial se habían impulsado nacionalismos y políticas segregacionistas en diversos territorios, como consecuencia los ánimos expansionistas resurgieron en el continente.

Durante esta época la Unión de Repúblicas Socialistas Soviéticas (URSS) contó con la mejor organización de inteligencia y espionaje del mundo. En 1934 el Directorio Político Unificado del Estado (OGPU) fue incorporado al Comisariado del Pueblo para Asuntos Internos (NKVD). Por su parte, la Dirección General de Seguridad del Estado (GUGB) y la cuarta sección militar de inteligencia lograron obtener datos valiosos como los mensajes intercambiados entre la embajada japonesa de Berlín y la de Praga. La GUGB también había monitoreado las negociaciones en Berlín entre el General Hiroshi Ōshima, más tarde nombrado embajador japonés, y el Ministro de Relaciones Exteriores de Alemania, Joachin Von Ribbentrop, que concluyeron en la firma del Pacto Anti-Komintern el 25 de noviembre de 1936 —que principalmente se oponía a la injerencia de la Internacional Comunista en los asuntos internos de otras naciones— de esta forma, Japón y Alemania formaron una alianza en la que se mantendrían informados sobre las actividades de la Komintern y se invitaría a otros Estados a adoptar medidas similares en contra de la Internacional Comunista.[27]

De lado alemán trabajaba la organización de inteligencia militar conocida como *Abwehr*, liderada por el Almirante Wilhelm Canaris, quien actuó como doble agente a favor de Alemania. *Abwehr* estaba a cargo de tropas, municiones, interceptar cables de telégrafo (y ondas de radio) y de la contrainteligencia militar. Entre los mayores logros de la organización

[26] *Ídem.*

[27] The Avalon Project, Documents in Law, History and Diplomacy. *Anti-Comintern Pact*. Yale Law School. [En línea]. Disponible en: <http://avalon.law.yale.edu/wwii/tri1.asp>. (Consulta 10/09/13).

está haber infiltrado a dos agentes en los organismos de inteligencia británicos y la creación de una excelente máquina criptográfica conocida como Enigma. La organización también se encargaba de interrogar a los prisioneros de guerra en busca de información significativa. En 1944 Heinrich Himmler, Jefe de la Policía Secreta Nazi mejor conocida como la *GESTAPO*, asumió el control de la organización, pues Wilhelm Canaris resultó el principal sospechoso de un atentado en contra de Hitler y altos funcionarios del gobierno alemán, Canaris y otros agentes fueron acusados de traición y ejecutados, poco después la *Abwher* se disolvió.[28]

Por parte de los servicios de inteligencia británicos, surgió la Dirección de Operaciones Espaciales que complemento las funciones del MI6.[29] Durante la Segunda Guerra Mundial existieron muchos miembros del MI6 que simpatizaban con el régimen nazi, incluso el jefe de las fuerzas aéreas de MI6 sostenía que Gran Bretaña y Alemania debían aliarse en contra de la URSS. Sin embargo, los objetivos de Alemania eran distintos. Gracias al trabajo de espías ingleses en Alemania el gobierno británico pudo enterarse de que se planeaba un ataque en su contra, poco después también arribaron reportes sobre un ataque a Polonia, no obstante los simpatizantes del régimen nazi desestimaron las pruebas por considerar que habían sido proporcionadas intencionalmente por judíos o bolcheviques que buscaban enemistar a ambas naciones.[30]

Otro de los casos de espionaje más sobresalientes de la Segunda Guerra Mundial es el de Harry Gold. Hacia 1940, el clima internacional se encontraba en un punto decisivo, pues las principales potencias habían iniciado una carrera armamentista que se enfilaba al desarrollo de la primera bomba atómica. Gold trabajaba para el gobierno estadounidense, pero simpatizaba con los ideales de la URSS, así que decidió intercambiar información militar estadounidense con la Unión soviética, la naturaleza de estos datos no era insignificante,

---

[28] Wilmoth Lerner, Adrienne. *Abwehr*. Espionage Information. Encyclpedia of Espionage, Intelligence and Security. [En línea]. Disponible en: <http://www.faqs.org/espionage/AAn/Abwehr.html>. (Consulta 10/09/13).

[29] Rama de los Servicios Secretos de Inteligencia que orientaba sus operaciones al exterior, mientras el MI5 trabaja al interior del país. Fuente: Security Service. (2012). "M16". *Politics.co.uk*. [En línea]. Disponible en: <http://www.politics.co.uk/reference/mi6>. (Consulta 25/09/13).

[30] Simkin, John. *Military Intelligence (MI6)*. Spartacus Educational. [En línea]. Disponible en: <http://www.spartacus.schoolnet.co.uk/FWWm6.htm>. (Consulta 25/09/13).

pues se trataba del desarrollo de la primera arma nuclear de la historia. Finalmente, Gold fue descubierto y condenado a 30 años de prisión.[31]

Con el fin de la Segunda Guerra Mundial concluye uno de los capítulos más lamentables de de la humanidad, la cantidad de víctimas (entre civiles y soldados) es sorprendente. El daño material, moral y económico que ocasionó en diversas naciones ha dejado vestigios que permanecen en la actualidad. Con la Conferencia de Yalta en febrero de 1945 los dirigentes de de Estados Unidos, Gran Bretaña y la URSS deseaban establecer orden en Europa, aunque para para algunos ese orden respondía a determinados intereses; meses después se estableció un nuevo mecanismo de cooperación internacional —la Organización de Naciones Unidas fue instaurada de manera oficial en octubre de 1945— para evitar que episodios tan sangrientos ocurrieran de nuevo en el mundo.[32] Sin embargo, la estabilidad tardó mucho tiempo en llegar a Europa, pues si bien el periodo posterior se caracterizó por la ausencia de un conflicto militar directo, la tensión y la desconfianza entre los miembros de la sociedad internacional serían constantes hasta finales del siglo XIX.

Durante la Guerra Fría los avances en la industria armamentista colocaron a los Estados en un escenario de tensión e incertidumbre, por esta razón diversas naciones impulsaron de forma importante el desarrollo científico-tecnológico en el ámbito de las comunicaciones con el fin de obtener datos valiosos sobre la capacidad militar del resto de los países, este periodo es conocido como la "época de oro del espionaje", pues el riesgo de un enfrentamiento con armas nucleares hizo de los servicios de inteligencia un elemento prioritario para la seguridad de cualquier nación. A diferencia de otras etapas de la historia, donde los avances en las técnicas de espionaje se dieron durante enfrentamientos militares, en la Guerra Fría el espionaje experimentó un momento de esplendor en un contexto de aparente estabilidad.

Las ideologías dominantes deseaban ampliar sus respectivas zonas de influencia, ante dicha situación se suscitaron una serie de enfrentamientos en diversos países, los episodios en donde

---

[31] Viana, Israel. (Octubre 2, 2013). Harry Gold, el espía "rechoncho" que entregó la bomba atómica a la URSS. *ABC.es*. [En línea]. Disponible en: <http://www.abc.es/20101210/archivo/harry-gold-espiaentrego201012091242.html>. (Consulta 20/10/13).

[32] Ayén Sánchez, Francisco. (2010). "La Segunda Guerra Mundial. Causas, desarrollo y repercusiones". (Sección Temario de oposiciones de Geografía e Historia), *Proyecto Clío 36*. [En línea]. Disponible en: <http://clio.rediris.es/n36/oposicones/tema70.pdf>. (Consulta 22/09/13).

un nuevo conflicto mundial estuvo a punto de estallar son significativos, y dichas tensiones proporcionaron múltiples oportunidades de acción para los organismos de inteligencia. esta época los servicios de inteligencia se encargaron de localizar, interrogar y eliminar a opositores de cada régimen. Un caso representativo de los servicios soviéticos es el de la operación WIN, después de la guerra las actividades estadounidenses antisocialistas en generaron toda una operación de contrainteligencia soviética. La operación WIN consistía en infiltrar agentes estadounidenses y disidentes del socialismo a Polonia para eliminar la influencia de la URSS. La operación WIN impulsada por la CIA fue todo un fracaso, pues al poco tiempo de haberse puesto en marcha fue descubierta. El gobierno de Polonia confesó que se trató de una trampa, pues WIN consistía en un plan para engañar a las potencias occidentales.[33]

Como este caso existen muchos más, ya que las agencias soviéticas formularon numerosas operaciones de la misma naturaleza en otros territorios como Ucrania y los países bálticos entre 1947 y 1952 con el fin eliminar grupos subversivos. En estas operaciones se crearon falsas fuerzas disidentes y operaciones para desinformar al enemigo, en resumen toda una táctica de contrainteligencia agresiva como lo describe Tennent H. Bagley (2007); de acuerdo con Oleg Kalugin, hacia finales de 1970 la KGB tenía agentes infiltrados en cincuenta organismos de inteligencia occidentales.[34]

Mientras tanto en Estados Unidos en plena carrera armamentística (1960), Allen Dulles y Richard Bissell dos colaboradores de la CIA solicitaron al congreso estadounidense el establecimiento de un programa de inteligencia que incluía el uso de aviones espía U-2 con el fin de obtener imágenes de plataformas para el lanzamiento de misiles balísticos intercontinentales situadas al norte de los Urales. El programa fue autorizado por el Presidente Dwight David Einsenhower, gracias a dicha operación el gobierno estadounidense descubrió el grado de desarrollo del programa soviético ICBM (por sus siglas en inglés *Inter-Continental Ballistic Missil*). Posteriormente Dulles y Bissel solicitaron la ejecución de nuevos programas en busca de más evidencias en contra de la Unión Soviética; sin embargo, las acciones de inteligencia estadounidenses fueron

[33] Suáres, Luis E. (Marzo 13, 2005). "General Reinhard Gehlen". *Exordio*. [En línea]. Disponible en: <http://www.exordio.com/1939-1945/militaris/espionaje/gehlen.html>. (Consulta 05/11/13).
[34] *Spy Wars*. (2007). Estados Unidos: Yale University Press. Citado por Tennet H. Bagley.

descubiertas el 1° de mayo de 1960 cuando el Ministro de Defensa de la URRS, Radion Malinovsky, le informó al Presidente Nikita Khrushchev que un avión U-2 había entrado al espacio aéreo soviético como respuesta el Presidente Khrushchev ordenó derribar la nave, aunque el gobierno estadounidense declaró que se trataba de un avión de investigación meteorológica, sus verdaderas intenciones habían sido descubiertas después de que las autoridades soviéticas inspeccionaran la nave. Estados Unidos no tuvo otra opción que aceptar su responsabilidad en el incidente; las consecuencias inmediatas fueron la cancelación de la Cumbre de París y la prohibición para sobrevolar el espacio aéreo soviético por parte cualquier aeronave estadounidense.[35] Debido a la medidas adoptadas por la URSS, Washington tuvo que acudir a otros métodos de inteligencia como el uso de satélites de reconocimiento dando inicio a una larga década de desarrollo de la industria espacial tanto en Estados Unidos como en la URSS, un periodo en el que los sistemas tecnológicos para la recolección de datos se enfocaron en el campo del desarrollo e investigación nuclear por parte de otras naciones.

Durante la Guerra Fría Estados Unidos y la URSS comenzaron a desarrollar aplicaciones científicas como sistemas avanzados de reconocimiento satelital, alarmas antimisiles, etc. Por lo que la década de los sesenta está caracterizada por la existencia de una extensiva y sofistica red de sensores tecnológicos capaz monitorear los avances de la industria militar y de inteligencia, de cualquier punto alrededor del globo.[36] Durante este periodo (antes de los cambios revolucionarios en la región) Estados Unidos mantenía estaciones SIGINT (inteligencia de señales) en Marruecos, Libia y Etiopia. Por otro lado, el gobierno estadounidense adoptó buques para la recolección de inteligencia que fueron utilizados por la NSA (Agencia de Seguridad Nacional) y la marina, específicamente dos tipos de barcos espía: el AGER[37] y el AGTR[38] con el objetivo de monitorear las bases navales soviéticas en Vladivostok, Corea del Norte, Cuba, y otras más en países de Sudamérica, el norte de África, y Medio Oriente, esta práctica surgió como respuesta al uso de barcos rastreadores con fines de espionaje por parte del gobierno soviético. Sin embargo, con el paso del tiempo las actividades de espionaje comenzaron a abarcar otros terrenos como el diplomático, un ejemplo de ello es la base estadounidense Menwith Hill (en Gran Bretaña) que bajo control de la NSA comenzó a

[35] Richelson. *Óp. Cit.*
[36] *Ídem.*
[37] Por sus siglas en inglés *Auxiliary General–Environmental Research*. (Barco Auxiliar de Investigación Ambiental).
[38] Por sus siglas en inglés *Auxiliary General –Technical Research*. (Barco Auxiliar de Investigación Técnica).

monitorear las comunicaciones diplomáticas de diversos países. Poco a poco los puertos de escucha se expandieron por el mundo al grado que Washington llegó a contar con siete bases inteligencia en Irán; dos de ellas en la costa este del Mar Caspio, dos en la costa sur, dos al noreste, y uno más en Behshahr.[39]

De esta forma, ante la ausencia de grandes conflictos bélicos como la Primera y Segunda Guerra Mundial y ante la creciente tensión por el dominio hegemónico, las medidas de protección de los Estados-nación se orientaran al campo de la inteligencia, enfocándose en uso del espionaje como medida preventiva, pues con ello se buscaba anticipar y evitar las acciones del enemigo. De esta forma, hacia finales del siglo XX las innovaciones en el campo de las tecnologías de la información y comunicación le otorgaron al espionaje nuevas áreas para desarrollarse, al tiempo en que se implementaron innovaciones en el ámbito del armamento militar que alcanzaron límites surrealistas.

1.1.5. La Era Informática

Con base en lo anterior se puede señalar que los avances en el dominio de la ciencia dieron paso a la aplicación de nuevas tecnologías en el ámbito de la industria militar y de inteligencia, carrera que (aunque no con la misma intensidad) prosigue hasta hoy en día, ya sea con el fin de recolectar información sobre áreas estratégicas de otras naciones, o para desarrollar sistemas defensivos y de ataque.

En las últimas décadas se ha experimentado una importante transformación en las comunicaciones, quizá la naturaleza de este cambio ha impedido notar el grado en que ha trasformado diversos estilos vida; sin embargo, basta comparar las formas de convivencia actuales con los métodos de comunicación de hace sólo 10 años. La evolución de las tecnologías de información y comunicación está avanzando a un ritmo cada vez más acelerado. De la misma forma en el ámbito internacional esta transformación ha afectado a las relaciones interestatales. Poco a poco, los Estados han adoptado nuevas formas de comunicación y organización al interior de su estructura, nuevos medios de interacción con la ciudadanía y nuevos canales de comunicación con el resto del mundo, del mismo modo la velocidad de dicha transformación ha impedido identificar sus fortalezas y debilidades.

[39] Richelson. *Óp. Cit.*

El uso de las TIC se ha convertido en una práctica esencial para la interacción entre naciones, dado que ningún país puede permanecer aislado del resto del mundo; sin embargo, la incorporación de estas herramientas demanda también nuevas medidas de protección, de esta forma podríamos resumir que: nuevos campos de convivencia incluyen también nuevas vulnerabilidades y nuevas amenazas.

En este aspecto es posible establecer que el desarrollo de las ciencias y sus aplicaciones potencializan la forma en que se puede dañar a una nación. Por un lado, la creciente dependencia hacia las TIC para el funcionamiento de los Estados quebranta su seguridad ante la posibilidad de un ataque cibernético, y por otro lado, está el avance de la industria armamentista, puesto que es capaz de transformar el beneficio de la ciencia en una amenaza. Empero, no es que el sistema internacional se encuentre al borde del colapso, sino que requiere de una transformación, de nuevas normas de convivencia y de nuevas formas de protección.

En los últimos años los casos de ciberespionaje han aumentado de forma importante en todo el mundo, las agencias de seguridad de diversas naciones se preocupan cada vez más por la seguridad cibernética de sectores clave ante la aparición de nuevas modalidades de ataque. Al respecto Martin Rudner (2013) ha analizado el riesgo que representan los ataques a la infraestructura crítica de las naciones e identifica al ciberespionaje como una amenaza potencial. Por esta razón, la confidencialidad de las bases datos y de los canales de comunicación se ha convertido en un tópico primordial en los organismos de seguridad, dado que la cantidad de datos que se pueden almacenar potencializa el daño que se puede causar a una nación. Ya sea en ámbito comercial, político, financiero, etc. el monitoreo y las sustracción ilícita de datos requieren de medidas de seguridad eficaces. En la arena internacional el espionaje cibernético entre naciones les muestra a los Estados que aunque el entorno es nuevo el objetivo sigue siendo el mismo: defender el interés particular.

Finalmente, es posible afirmar que la guerra y el espionaje son actividades que de forma ineludible han acompañado al hombre desde que comenzó a escribir su historia. En particular, el espionaje constituye una herramienta estratégica para las naciones en búsqueda de dominio territorial, económico, político e ideológico, pues a lo largo del tiempo diversos Estados han adoptado tanto instrumentos como actividades ilícitas en su búsqueda por alcanzar el dominio hegemónico.

En los últimos años la evolución de la ciencia y las comunicaciones le ha otorgado a la industria militar nuevas herramientas para la defensa y protección de las naciones, pero también han aparecido nuevas técnicas ofensivas, en este aspecto los ataques cibernéticos constituyen una de las grandes amenazas del siglo XXI, ya que representan formas de combate para las que la sociedad internacional aún no está preparada, muestra de ello son los casos de ciberespionaje que se analizan a continuación que demuestran la falta de medidas adecuadas —tanto en el plano técnico como jurídico— para responder a esta clase de amenazas.

1.2. Casos de ataques informáticos

La idea de un enfrentamiento entre naciones caracterizada por el uso de herramientas tecnológicas no es nueva, pues hacia finales del siglo XX diversos teóricos se dedicaron a analizar dicho escenario.[40] En este sentido la adopción de innovaciones tecnológicas en el campo del espionaje es, sin duda, una práctica circunscrita en el planteamiento de una ciberguerra. Por esta razón, los avances tecnológicos que sorprendieron a la sociedad a finales del siglo pasado, y principios del presente, también preocuparon a las naciones, pues representan la necesidad de actualizar los mecanismos de regulación y protección de las comunicaciones interestatales.

Como se observó en el apartado anterior, el desarrollo de herramientas tecnológicas en la práctica del espionaje se dio con mayor medida durante el periodo de Guerra Fría y desde entonces los avances en este campo son cada día más impresionantes. En el plano internacional las agencias de inteligencia y los organismos de seguridad no han permanecido indiferentes, sino al contrario han buscado fortalecerse con el uso de esas nuevas herramientas. Sin embargo, la accesibilidad y estructura de la red es capaz desvanecer cualquier ventaja, pues se han presentado diversos casos en donde los ataques informáticos sobrepasan la capacidad de defensa de los Estados-nación.

---

[40] Entre los trabajos más significativos se encuentran: Wang Qingsong, *Modern Military-Use High Technology* (1993); Zhu Youwen, *Information War under High Tech Conditions* (1994), Li Qingshan, *New Military Revolution and High Tech War* (1995), entre otros. Del lado occidental aparecieron trabajos como: *Technology and War* (1991) de Martin Van Creveld; *The First Information War* (1992) de Alan D. Campen; *The Advent of Netwar* (1996) de John Arquilla, entre otros.

1.2.1. El caso Shawn Carpenter

En 2004 se registró el primer caso de espionaje cibernético en la historia y el cual consistía en una enorme red que operaba en contra de diversas entidades estadounidenses. Shawn Carpenter trabajador del Laboratorio Nacional de Sandia en Albuquerque, Nuevo México, descubrió una operación de ciberespionaje procedente de China, que logró introducirse en el sistema de Sandia, en instalaciones militares, en compañías subcontratistas de seguridad y en agencias gubernamentales de las que robó información clasificada relacionada con el sistema de defensa antimisiles estadounidense y con la misión de reconocimiento espacial a Marte de la Administración Nacional de la Aeronáutica y del Espacio, NASA (por sus siglas en inglés). Carpenter intentó detener las operaciones que atacaban al Laboratorio Nacional; sin embargo, sus acciones le ocasionaron serios problemas. Todo comenzó en verano de 2003 cuando fue asignado a un equipo especial encargado de investigar intrusiones en los sistemas informáticos de la corporación Lockheed, gracias ello Carpenter descubrió que el Laboratorio Nacional de Sandia también estaba siendo atacado por una de las tantas direcciones electrónicas identificadas en el ataque a Lockheed. Poco a poco, el ahora ex colaborador de Sandia descubrió la magnitud de las operaciones, pues como resultado de la investigación anterior Carpenter podía acceder a las herramientas que los hackers utilizaban para introducirse en otras redes, y conocer los datos que habían sido robados. De acuerdo con Richard Stiennon (2010) esta operación logró sustraer cientos de archivos de entidades militares, comerciales y de investigación de Estados Unidos. Cuando Shawn Carpenter informó a sus superiores del alcance de las operaciones fue ignorado, de manera que acudió a un contacto en el ámbito de la contrainteligencia militar con el que colaboró durante tres meses para detener la amenaza cibernética; no obstante, cuando las autoridades de Sandia se enteraron de su participación decidieron removerlo de su cargo por insubordinación, Carpenter no recibió respaldo de ninguno de los organismos a los que ayudó (el FBI y la *Army Research Labs Center for Intrusion Monitoring and Protection*). También conocido como "Titan Rain" este caso es recordado porque evidenció la debilidad de los sistemas informáticos de las estructuras estatales estadounidenses, así como la escaza coordinación entre las autoridades encargadas de castigar esa clase delitos

1.2.2. El virus Haephrati

Poco después del incidente en los laboratorios de Sandia apareció el virus troyano Haephrati, el cual representa uno de los más famosos casos de espionaje cibernético en el ámbito industrial (registrado en 2005). El *malware* fue creado por Michael Haephrati y Ruth Brier-Haephrati, quienes más adelante se dedicaron a ofrecer el virus a agencias privadas de investigación (de origen israelí) con el fin de instalarlo en los equipos de cómputo de la competencia. Pese a que las autoridades de Tel Aviv lograron descubrir la operación de espionaje el virus Haephrati logró sustraer miles de documentos confidenciales con alto valor comercial de diversas empresas. Las víctimas del ataque pertenecían al sector de la telefonía y de transmisión de televisión vía satelital, aunque afortunadamente en esta ocasión se logró detener a los responsables, el caso demostró la vulnerabilidad de los sistemas informáticos, pues el software malicioso operó, por lo menos, durante dos años y medio sin que ningún programa antivirus lograra detectarlo.[41]

1.2.3. La Operación ShadyRAT

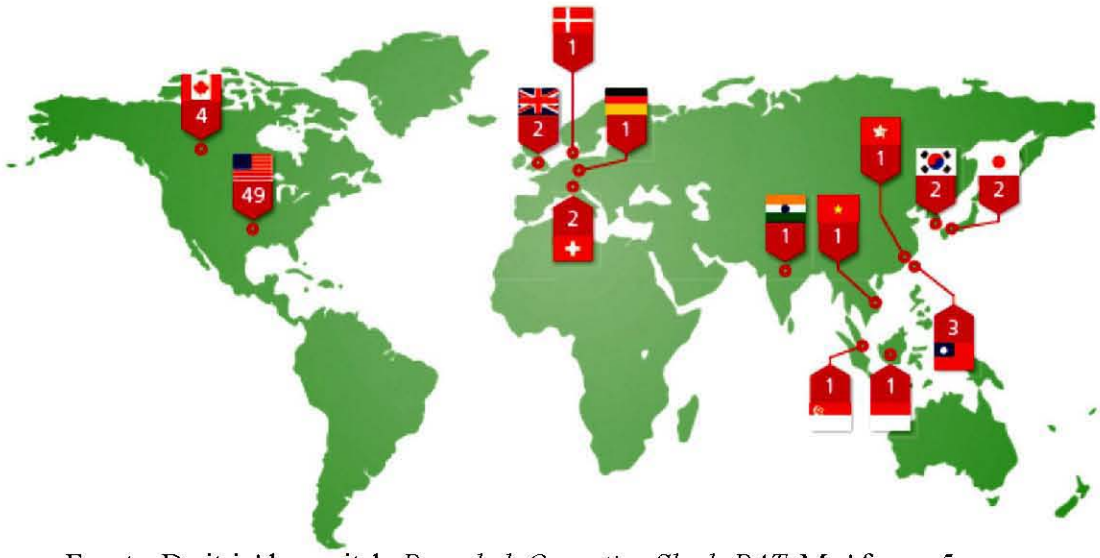
En 2008 comenzó a ejecutarse una de las más grandes operaciones de ciberespionaje en la historia, en esta ocasión las pruebas de nuevo apuntan hacia China. El caso fue investigado por la compañía McAfee quien decidió nombrarlo "operación ShadyRAT".

ShadyRAT constituye un gran desafío a los mecanismos de protección de datos. Según, Dmitri Alperovitch (autor del informe McAfee) la operación inició poco antes de los Juegos Olímpicos organizados por la República Popular de China, y su principal objetivo era recolectar información relacionada con seguridad nacional, bases de datos, correos electrónicos, planes de negocios, contratos, entre otros datos confidenciales. La operación atacó a 43 organizaciones localizadas en 13 países (véase mapa 1), entre los organismos afectados figuran: departamentos de energía, empresas de bienes raíces, entidades comerciales tanto asiáticas como occidentales, y la Asociación de Naciones del Sudeste Asiático, ASEAN (por sus siglas en inglés). Progresivamente los objetivos de ShadyRAT fueron aumentando, incluyendo empresas privadas relacionadas con seguridad nacional (de

[41] Agencia EFE. (Mayo 30, 2005). "Espionaje industrial en Israel a través de troyanos". *ABC.es*. [En línea]. Disponible en:<http://www.abc.es/hemeroteca/historico-30-052005/abc/Ultima/espionaje-industrial-en-israel-a-travesdetroy anos_202820039620.html>. (Consulta 05/10/13).

Estados Unidos), organismos en Vietnam, compañías de seguridad cibernética, entre otros. En 2008, la operación afectó a la Organización de Naciones Unidas y la Agencia Mundial Antidopaje, AMA. El mecanismo consistía enviar un correo electrónico infectado a los empleados de las organizaciones seleccionadas, de esta forma se instalaba un comando de acceso remoto al ordenador, a través del cual se conseguía acceso a todos los archivos.[42] Una de las principales características de este tipo de ataque es el anonimato, ya que aunque se ha logrado identificar y detener la operación, la identidad del agresor, hasta el día de hoy, es desconocida. Aunque las pruebas señalan al gobierno chino, no es claro si efectivamente fue el origen del ataque o simplemente es utilizado para cubrir la identidad del agresor. Esta situación convierte al espionaje cibernético en uno de los delitos más efectivos, pues en la mayoría de los casos es capaz de causar daño sin que el culpable sea sancionado.

Mapa 1. Localización geográfica de los objetivos de ShadyRAT



Fuente: Dmitri Alperovitch. *Revealed: Operation Shady RAT*. McAfee, p. 5

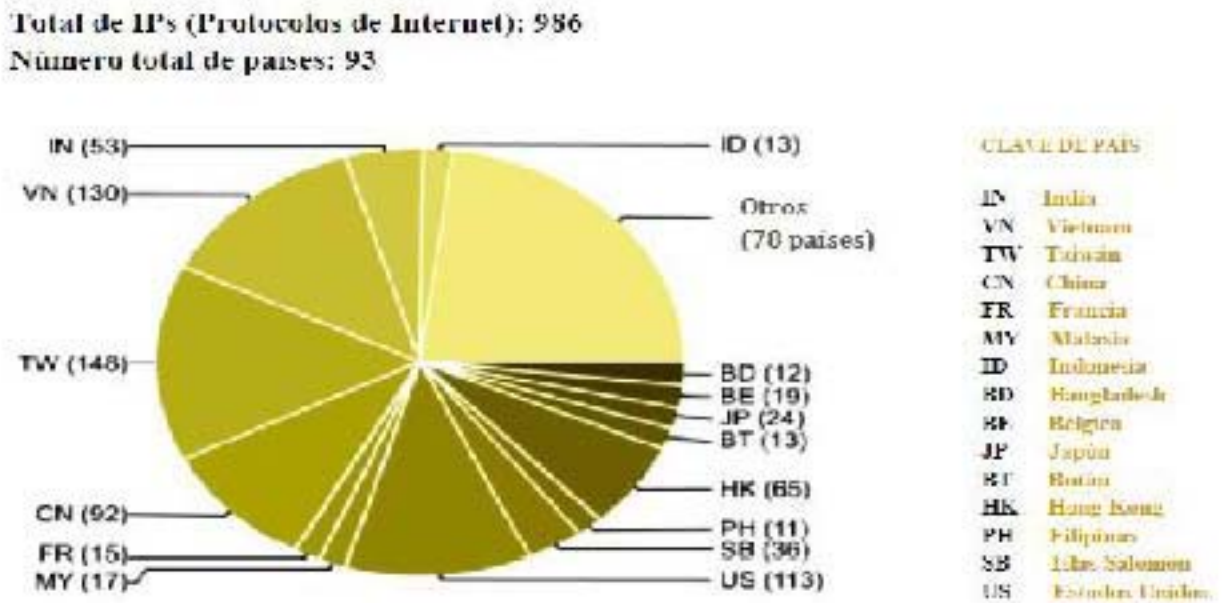
1.2.4. La Red Ghosnet

En los últimos años los casos en los que la República Popular China es identificada como el origen de las agresiones han aumentado. En 2009 investigadores del Centro Munk de estudios internacionales de Universidad de Toronto revelaron la existencia de una gran red de ciberespionaje que se relacionaba con China. La red conocida como Ghostnet, logró

[42] Alperovitch, Dmitri. *Revealed: Operation Shady RAT*. McAfee. [En línea]. Disponible en: <http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf>. (Consulta 23/10/13).

introducirse en 1 300 computadoras pertenecientes a por lo menos 103 países, de las cuales robó información con alto valor diplomático, político, económico y militar. La información sustraída pertenecía Ministerios de exterior, embajadas, a la oficina central de la OTAN, y a oficina del dirigente del Gobierno tibetano en el exilio (intrusión que dio origen a toda la investigación). Entre los sistemas afectados estaba el correo electrónico del Dalai Lama de donde sustrajeron unas 1500 cartas entre enero y noviembre de 2009 –de acuerdo con el estudio realizado por el Centro Munk publicado en 2010.[43] Según los investigadores de la Universidad de Toronto el treinta por ciento de los equipos afectados contenía información considerada como altamente confidencial, pues pertenecía a organizaciones como la ASEAN, al Banco Asiático de Desarrollo, a las Oficinas de Exterior de Indonesia y Filipinas, a diversas embajadas de países como Chipre, Alemania, India, Malta, Portugal, Rumania, Tailandia, entre otros, y a organizaciones no gubernamentales (véase gráfica 1). La operación Ghostnet trabajó sin que ninguna organización o gobierno lo sospechara durante casi dos años.[44]

Gráfica 1. Localización geográfica y número de sistemas infectados por *Ghostnet*



Fuente: *Tracking Ghostnet: Investigating a Cyber Espionage Network.* Information Warfare Monitor. Marzo 29, 2009. Canadá, pp. 41.

[43] Moore, Malcolm. (Abril 6, 2010). "Chinese hackers steal Dalai Lama's emails". *The Telegraph*. [En línea]. Disponible en: <http://www.telegraph.co.uk/news/worldnews/asia/china/ 7559103/Chinese-hackers-steal-Dalai Lamas-emails.html>. (Consulta 23/10/13).

[44] Information Warfare Monitor. (Marzo 29, 2009). *Tracking GhostNet: Investigating a Cyber Espionage Network*. Munk Centre for International Studies, University of Toronto. [En línea]. Disponible en: <http://www.nartv.org/mirror/ghostnet.pdf>. (Consulta 23/10/13).

1.2.5. Mossad *versus* Siria

Otro caso importante de ciberespionaje surgió en noviembre de 2010 cuando la revista alemana *Der Spiegel* reveló la historia de la destrucción de instalaciones nucleares Sirias por parte de Israel. Todo comenzó cuando un importante oficial sirio hospedado en Londres fue perseguido por los servicios de inteligencia israelí (Mossad), en esta ocasión la operación combinó ingeniería humana y ciberespionaje, ya que en cuanto el representante sirio salió del hotel agentes israelíes irrumpieron en la habitación e introdujeron un software malicioso en su ordenador portátil. Según *Der Spiegel* el gobierno israelí consiguió datos altamente confidenciales sobre centros de desarrollo e investigación nuclear en Siria, y descubrió la relación de dicho gobierno con el programa nuclear de Corea del Norte. Posteriormente Israel lanzó un ataque que aniquiló las instalaciones nucleares sirias. Según Richard Stiennon (2010) las prácticas de ciberespionaje israelíes son ampliamente conocidas, y al mismo tiempo Israel también es objeto de numerosos ataques por parte de grupos islamistas.

1.2.6. La Operación Aurora

Hasta este momento, aunque la sociedad internacional ya era consciente del riesgo de un ataque cibernético no había conocido la magnitud de sus alcances, pues un importante programa de espionaje se estaba ejecutando de forma silenciosa en el ciberespacio. Entre las víctimas del atentado se encuentra el reconocido buscador web *Google*. La operación Aurora es una de las más grandes redes de espionaje internacional, ya que logró burlar la seguridad de un sin número prestigiadas empresas. El caso salió a la luz cuando, en enero de 2010, colaboradores de *Google* revelaron haber recibido correos sospechosos invitándolos a visitar una misteriosa dirección electrónica, acto seguido un *malware* fue introducido en sus ordenadores. Aurora es conocida como uno de los ataques cibernéticos más sofisticados, y hasta el día de hoy se desconoce la cantidad de datos que lograron sustraerse, así como el número de empresas que fueron perjudicadas. La investigación judicial indica que el servidor desde donde se lanzó la ofensiva se localizaba en China; sin embargo, la naturaleza de Aurora

impide conocer al cien por ciento el origen del ataque, de ahí que constituya un verdadero enigma para los expertos en el campo informático.[45]

A diferencia de las prácticas de espionaje utilizadas en el siglo XX, el espionaje electrónico representa una amenaza significativa, pues opera en un espacio intangible compuesto por cientos de redes interconectadas; de manera que los métodos con los que se puede irrumpir en un sistema informático se multiplican de forma exponencial. Por lo tanto, el descubrimiento de puertas de acceso y debilidades en un sistema convierten al ciberespionaje en una actividad prácticamente imperceptible dado que en el ciberespacio es casi imposible ejercer control absoluto. En adición, el desarrollo tecnológico ofrece cada día mejores herramientas para la ejecución de esta clase de ataques, al tiempo en que surgen nuevos grupos subversivos cuyo domino de las TIC representa un verdadero desafío para la seguridad de las naciones.

1.2.7. China *versus* Canadá

En 2011 la prensa canadiense dio a conocer una serie de operaciones de ciberespionaje en contra de organismos estatales relacionados con seguridad y economía. Desde enero de ese mismo año las autoridades ya habían detectado la sustracción ilícita de información e intentaban erradicarla. El origen nuevamente conducía a la República Popular China. La operación irrumpió y robó información del sistema financiero y de hacienda, que constituye uno de los pilares de la nación. Respecto a las autoridades no hubo ninguna declaración del entonces Primer Ministro Stephen Harper; del caso sólo se emitió un comunicado en el que se aseguró que se trataba de un intento por ingresar a los sistemas gubernamentales. Por su parte, el gobierno de la República Popular China, declaró que no tenía ninguna responsabilidad en dicho atentado. Según la prensa canadiense, el objetivo era obtener contraseñas de los sistemas gubernamentales para conseguir control total, con ello los ciberespias también obtendrían acceso a información personal de miles de ciudadanos.[46]

---

[45] Acosta, Nelly. (Enero 20, 2010). "'Operación Aurora', el ciberataque más sofisticado de la historia". *El Economista*. [En línea]. Disponible en: <http://eleconomista.com.mx/tecnociencia/2010/01/20/operacion-aurora-ciberataquem as-sofisticado-historia>. (Consulta 23/10/13).

[46] Weston, Greg. (Febrero 16, 2011). "Foreign hackers attack Canadian government". *CBCnews*. [En línea]. Disponible en: <http://www.cbc.ca/news/politics/foreign-hackers-attack-canadian-government-1.982618>. (Consulta 29/10/13).

Como es posible observar las operaciones en donde la República Popular China está involucrada son numerosas; sin embargo, como también se ha mencionado la naturaleza de esta clase de ataques impide determinar con toda certeza el origen de la operación. Al respecto existen múltiples opiniones, lo cierto es que los casos antes mencionados no hacen más que evidenciar la debilidad del sistema internacional en la materia, ya sea en el plano jurídico o técnico la necesidad de establecer nuevos mecanismos es urgente. Es preciso recurrir a la cooperación internacional para establecer organismos y medidas que tipifiquen y sancionen prácticas de ciberespionaje, pues dada la universalidad de la web es necesario que todas las naciones colaboren en esta tarea. No obstante, el panorama resulta poco alentador, ya que en los últimos años ha surgido una serie de reclamos por parte de determinados países acusándose mutuamente de cometer espionaje cibernético (principalmente Estados Unidos, Rusia y China).

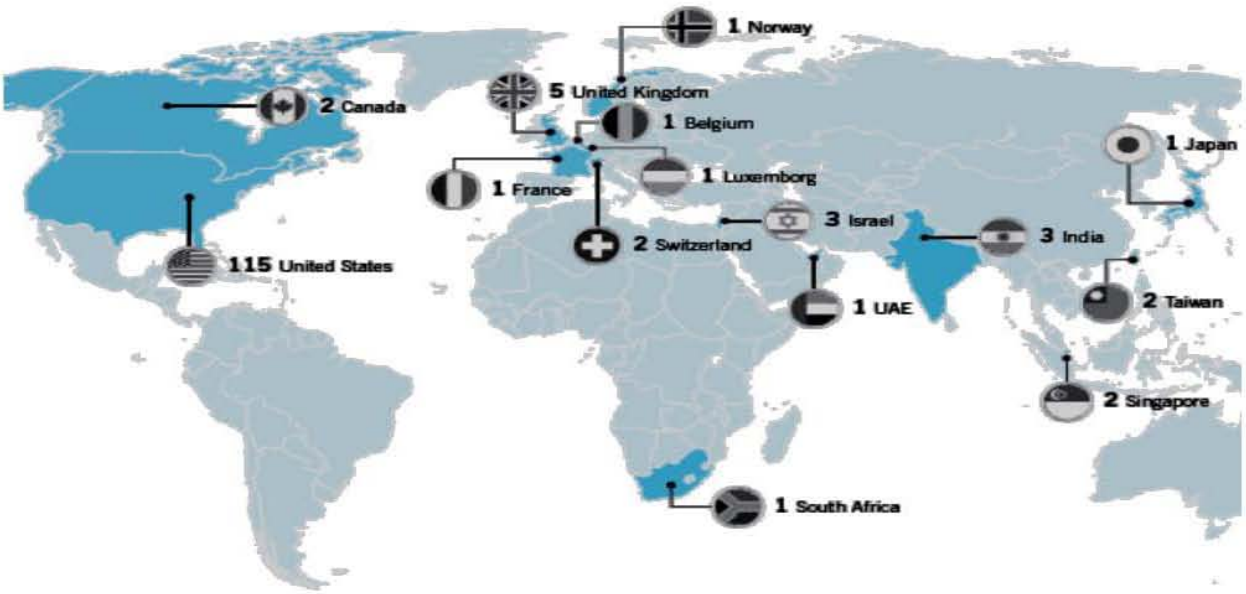
1.2.8. La Red ATP1

Respecto a lo anterior vale la pena analizar el reporte elaborado por la compañía estadounidense Mandiat,[47] en donde se describe la metodología y composición de la unidad de ciberespionaje del gobierno chino. La compañía afirma (con base en los resultados del informe) que el gobierno chino autoriza y apoya las operaciones de ciberespionaje, aunque —según Mandiat— no existe evidencia concreta al respecto. De acuerdo con el estudio, la red de espías cibernéticos opera desde 2006 y forma parte del Ejército Popular de Liberación, específicamente de la Unidad 61398 compuesta por cientos de trabajadores. Uno de los datos en los que Mandiat basa su argumento es que la compañía estatal de comunicaciones *Telecom* provee de fibra óptica especial e infraestructura a la Unidad 61398, cuyas actividades son consideradas secreto de Estado. La operaciones detectadas por Mendiat afectaron a 141 organizaciones de las que sustrajeron cientos de terabytes de información (un terabyte equivale a 1 000 000 de gigabytes) durante aproximadamente cinco años. Respecto a los objetivos, estos se localizaron de forma especial en Estados Unidos, Canadá, Reino Unido y diversas organizaciones cuyo idioma principal es el inglés, aunque también afectaron organizaciones que utilizaban algún otro idioma (véase mapa 2). Los sectores a los que pertenecían dichos organismos van desde las comunicaciones hasta la agricultura. Dada la extensión de las

[47] Mandiant. *APT1, Exposing One of China's Cyber Espionage Units*. [En línea]. Disponible en: <http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf>. (Consulta 29/10/13).

actividades, así como la dificultad para identificarlas, algunos medios se han referido a esta misma red con nombres como "Comment Crew" y "Comment Group" a menudo se ha una conexión con las redes *ShadyRAT* y *Aurora*, sin embargo sólo ésta última posee relación con la red ATP1 —por sus siglas en inglés, Amenazas Persistentes Avanzadas—, nombre designado por Mendiat. (Véase mapa 2).

Mapa 2. Localización geográfica de las víctimas de ATP1



Fuente: *APT1, Exposing One of China's Cyber*. MENDIAT. 2013, pp. 22

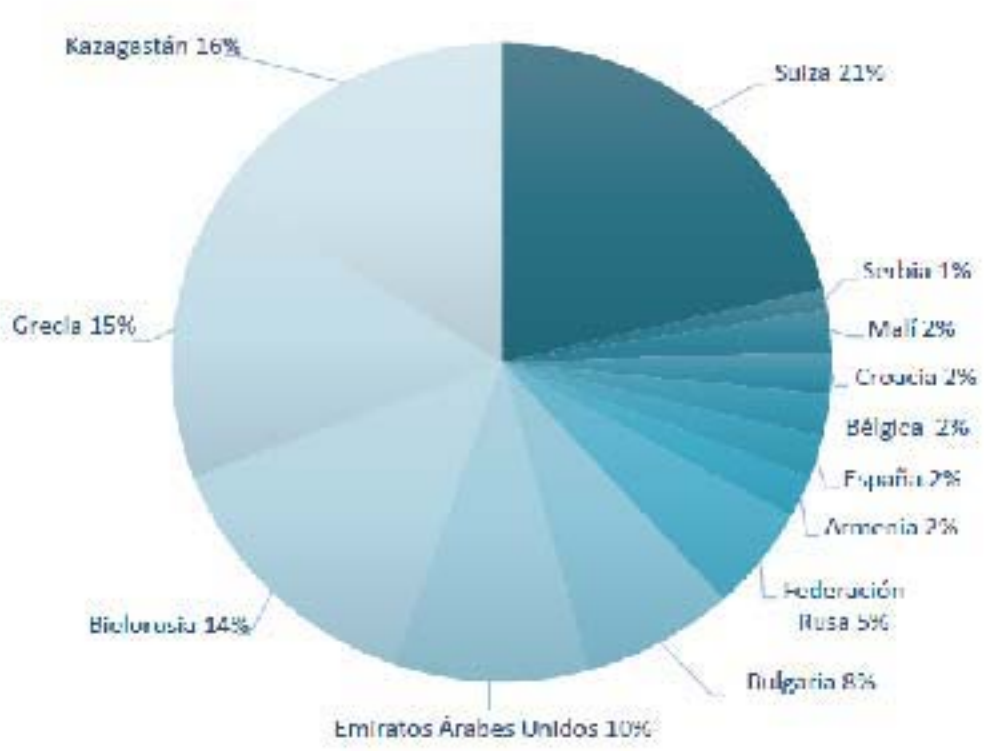
1.2.9. La Operación Octubre Rojo

Por otra parte, está la operación Octubre rojo descubierta en 2012. El mecanismo utilizado es uno de los más complejos que se han conocido y fue diseñado especialmente para atacar embajadas, organismos de la industria aeroespacial, organizaciones militares, entidades comerciales, centros de investigación energética y nuclear, y compañías de gas y petróleo de aproximadamente 39 naciones (véase gráfica 2).[48] La operación consistía en: sustraer datos, registrar el uso de teclas, robar contraseñas, extraer información de cuentas de correo electrónico e historiales de navegación así como recolectar datos de lápices

[48] Kaspersky Lab. (Enero 14, 2013). *"Red October" Diplomatic Cyber Attacks Investigation*. Securelist. [En línea]. Disponible en: <http://www.securelist.com/en/analysis/204792262/Red_October_Diplomatic_Cyber_Attacks_Investigation>. (Consulta 05/11/13).

electrónicos, teléfonos móviles, etc.[49] El tipo de datos que el *malware* era capaz de robar incluía la extensión *.acid* que es utilizada por el software *Acid Cryptofiler* uno de los programas programas de cifrado que utiliza la OTAN. Dada las funciones del software malicioso se cree cree que las víctimas del ataque habían sido perfectamente delineadas. De acuerdo con Kaspersky Lab (entidad encargada de la investigación) los primeros reportes aparecen 2007 mientras que la última actividad se registró en enero de 2013.

Gráfica 2. Distribución geográfica de ciberataques de la operación *Octubre Rojo*



Fuente: *"Red October" Diplomatic Cyber Attacks Investigation*. Security Analyst Summit 2014.

1.2.10. El caso PRISMA

Sin duda alguna el caso que ha logrado impactar a la sociedad internacional es el programa PRISMA. Revelado el 7 junio de 2013 por el ex analista militar Edward Snowden[50], quien

[49] De los Santos, Sergio. (Enero 17, 2013). "Operación octubre rojo: un malware muy 'personal'". *Hispasec*. [En línea]. Disponible en: <http://unaaldia.hispasec.com/2013/01/operacion-octubre-rojo-un-malware-muy.html>. (Consulta 05/11/13).

[50] Pérez Silva, Ciro. (Julio 2, 2013). "México trata de manera directa con EU las 'presuntas filtraciones': SRE". *La Jornada*, p. 3.

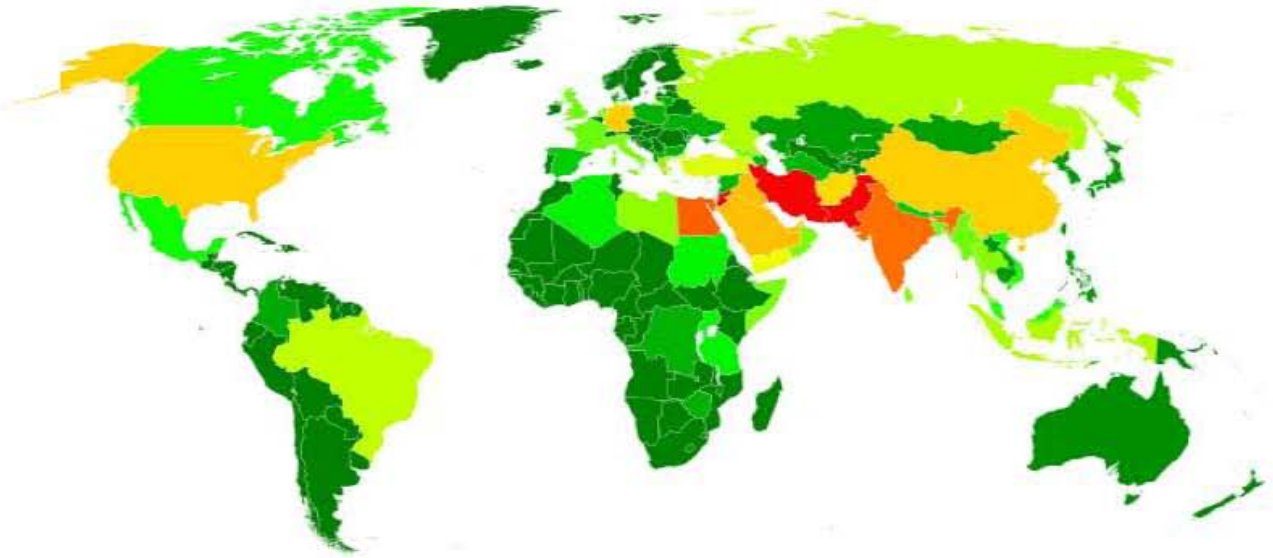
trabajó para la empresa Booz Allen Hamilton subcontratista de la Agencia Nacional de Seguridad, NSA (por sus siglas en inglés). En esta ocasión el rumbo de las acusaciones dio giro radical, pues el programa PRISMA, que consiste en una enorme operación de ciberespionaje, es llevada a cabo por el gobierno estadounidense. Snowden ha declarado que las autoridades de Washington ayudadas por otros organismos de inteligencia se encargan de recolectar información de cualquier parte utilizando todos los medios posibles. De esta forma agencias como la NSA son capaces de sustraer información de cualquier persona. Para el ex analista, las acciones de Estados Unidos atentan contra la democracia, por lo que decidió revelar su identidad, ya que rechaza abiertamente la forma en la que las autoridades abusan del poder.[51] El programa revelado por Snowden consta de dos herramientas, la primera es conocida como *boundless informant* un software capaz recolectar, contabilizar y esquematizar datos provenientes de líneas telefónicas y equipos de cómputo de todo el mundo (véase mapa 3). Los documentos facilitados por Snowden muestran que *boundless informant* recolectó tres mil millones de reportes de inteligencia durante un periodo de sólo 30 días. La herramienta ordena y mapea una enorme cantidad de datos pertenecientes a operaciones de inteligencia estadounidenses en diversos países a fin de agilizar las operaciones. Entre los Estados más monitoreados figuran Irán, Pakistán, Jordania, Egipto e India.[52] La siguiente herramienta es quizá la más conocida, pues ha servido para identificar los mecanismos de espionaje cibernético de Washington, su nombre es PRISMA y consiste en un software encargado de obtener información de correos electrónicos y servicios de mensajería instantánea de importantes compañías como *Google*, *Facebook*, *Skype*, *Apple*, *Microsoft*, entre otras. Es importante apuntar que el programa exigía el acceso a la información de los usuarios de dichas compañías, por lo que éstas eran conscientes de la intrusión de PRISMA, de acuerdo con lo declarado por Snowden. Según el diario británico *The Guardian* —a quien el ex analista proporcionó la información— el programa opera

[51] Greenwald, Gleen y Laura Potras. Traducción de Leonardo Boix. (Julio 14, 2013). "Los motivos de Snowden". *Proceso*, No. 1915, pp. 50-55.

[52] Greenwald, Gleen y Ewen MacAskill. (Junio 11, 2013). "Boundless Informant: the NSA's secret tool to track global surveillance data". *The* Guardian. [En línea]. Disponible en: <http://www.theguardian.com/world/2013/jun/08/nsaboundless-informant-global-datamining#>. (Consulta 05/11/13).

desde 2007 como parte de las reformas a las leyes de seguridad y vigilancia implementadas por George W. Bush. [53]

Mapa 3. Áreas monitoreadas por el programa *Boundless Informant* de la NSA



Los rangos de color verde muestran las zonas menos vigiladas, aumentando a amarillo y naranja hasta rojo que representa las áreas más monitoreadas (al 2007).

Fuente: Glenn Greenwald y Ewen MacAskill. "Boundless Informant: the NSA's secret tool to track global surveillance data". *The Guardian*, 11 de junio de 2013.

Con estas revelaciones Snowden también destapó toda una operación de ciberespionaje orquestada por Washington en contra de 38 embajadas y misiones diplomáticas de países como Francia, Grecia, Italia, Japón, México, Corea del sur, India, Turquía y representaciones de la Unión Europea y la Organización de Naciones Unidas.[54]

Con todo lo anterior, el porvenir del sistema político internacional parece un tanto indescifrable, pues es difícil determinar las acciones que adoptaran los Estados-nación para proteger la privacidad de sus comunicaciones. Por un lado, se ha desatado una ola de reclamos por parte de diversas naciones contra Washington como consecuencia de las revelaciones de Snowden. En este aspecto el debate oscila entre quienes plantean al espionaje como una

[53] Morris, Nigel. (Junio 7, 2013). "Q&A: What is Prism, what does it do, is it legal and what data can it obtain?" *The* Independent. [En línea]. Disponible en: <http://www.independent.co.uk/news/world/americas/qa-what-is-prismw hat-does-it-do-is-it-legal-and-what-data-can-it-obtain-8650239.html>. (Consulta 10/11/13).

[54] Alcaraz, Yetlaneci. (Julio 14, 2013). "Hipocresía europea". *Proceso*, No. 1915, pp. 52-55.

actividad recurrente en el ámbito de las relaciones internacionales, y los que condenan las violaciones al Derecho Internacional del país "portavoz" de la democracia.

Por otro lado, están los que abogan por establecer acuerdos internacionales en la materia, en este sentido el panorama no es claro, pues con el surgimiento de diversos escándalos de ciberespionaje internacional inevitablemente se han fracturado las relaciones entre los Estados. Ante esta situación el escenario más factible es que se establezcan normas y organismos que tipifiquen y sancionen el espionaje cibernético a nivel regional, bilateral o nacional, pues la comunidad internacional se enfrenta al desafío de renovar la confianza entre sus componentes para establecer mecanismos que respondan a una realidad caracterizada por el incesante avance de las nuevas tecnologías.

Resulta interesante observar como en plena Era informática, el principal riesgo recae en la privacidad de la información. La apertura de las comunicaciones coloca a las naciones en la disyuntiva de aceptar el uso de nuevos medios y dar la bienvenida a la sociedad del conocimiento o restringir su uso para proteger las comunicaciones internas y externas, punto que suele enfrentarse con el respeto a los derechos y libertades de sus ciudadanos. Sin embargo, como se ha observado las nuevas tecnologías y en especial la web representan una herramienta de doble filo, pues la adopción de nuevos canales de comunicación trae consigo nuevas formas en las que se puede dañar a una nación, el dilema reside en restringir el uso de herramientas tecnológicas que resultan esenciales para el funcionamiento de cualquier nación o formar parte de la aldea global en donde la seguridad de las comunicaciones internacionales reside en la voluntad de los Estados para cumplir las normas del Derecho Internacional.

1.2.3. Convenciones sobre ciberespionaje

Dado que la sociedad es un elemento del Estado en constante transformación, las normas que regulan su comportamiento se encuentran permanentemente en proceso de renovación. En el plano internacional el establecimiento de reglas consiste en un mecanismo de mayor complejidad, pues ante la ausencia de una entidad supranacional que garantice el pleno cumplimiento de las normas el respeto a las leyes recae en la voluntad de los Estados. Esta voluntad puede verse influenciada por la clase de relaciones entre las naciones, así como de

sus respectivos intereses. En el ámbito de la seguridad el cumplimiento de las normas del Derecho Internacional representa un elemento esencial para la estabilidad del sistema mundial.

En este aspecto pese a la enorme propagación del uso de nuevas tecnologías, aún no existen acuerdos internacionales en la materia. En cuanto al espionaje se han establecido diversos instrumentos encargados de sancionarlo; sin embargo, es necesario actualizar —o establecer— medidas apropiadas en el caso del ciberespionaje, pues debido su naturaleza posee un potencial significativamente mayor. Como se ha observado existen diversos mecanismos para sustraer, alterar e interceptar información que circula en el ciberespacio, aunado a ello la cantidad de datos que se ubican y circulan en la red de redes es exorbitante, por esta razón la necesidad de proteger las comunicaciones oficiales es urgente.

Al tiempo en que surgen nuevos medios físicos y virtuales para compartir, depositar o transferir datos, también son cada vez más numerosos los ataques cibernéticos y operaciones de espionaje informático en todo el mundo. Sin embargo, existen importantes esfuerzos orientados a la regulación de las TIC, por lo que vale pena examinarlos, impulsar su actualización y, de ser necesario, establecer nuevos instrumentos jurídicos en la materia.

El convenio sobre ciberdelicuencia de la Unión Europea (celebrado en 2001 y que entró en vigor en 2004) es uno de los esfuerzos más significativos, pues se trata del primer instrumento internacional en la materia. El convenio firmado en Budapest establece en el capítulo segundo las medidas que deben adoptarse para castigar delitos contra la confidencialidad, la integridad y la disponibilidad de datos y sistemas informáticos tomando en cuenta acciones como acceso e intercepción ilícita, y ataques contra datos y sistemas informáticos de los países miembros. Por lo que la comunidad europea hace un llamado a las partes que la integran para adoptar las medidas legislativas necesarias que les permitan cumplir con lo estipulado en el convenio, también reconoce el carácter esencial de la cooperación internacional para el seguimiento de dichos objetivos.[55] Es importante señalar que la Unión Europea lanza una invitación para que otros Estados (no miembros de la Unión) puedan adherirse a dicho convenio; en 2009 Canadá, Estados Unidos, Japón y Sudáfrica se unieron al esfuerzo europeo, firmando el acuerdo.

[55] Consejo de Europa. (Noviembre 23, 2001). *Convenio sobre la Ciberdelicuencia*. Serie de Tratados Europeos, no. 185. [En línea]. Disponible en: <http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Convention%20and%20protocol/ETS_185_spanish.PDF>. (Consulta 11/11/13).

Adicionalmente, el instrumento también ha servido como modelo para que otras naciones como Argentina, Botsuana, Egipto, Filipinas, Nigeria y Pakistán modifiquen sus legislaciones para castigar esta nueva clase de infracciones.[56] Para reforzar lo anterior en 2009 se emitió la Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones sobre protección de infraestructuras críticas de información bajo la denominación "Proteger Europa de ciberataques e interrupciones a gran escala: aumentar la preparación, seguridad y resistencia" en donde la Comisión Europea identifica la vulnerabilidad de las infraestructuras criticas ante las amenazas cibernéticas y el enorme riesgo de una interrupción a gran escala.[57] Lo más importante es que el papel de la Unión Europea no sólo se limitó al campo jurídico, pues que tras la aprobación del Parlamento y del Consejo Europeo en 2005 la Agencia Europea de Seguridad de las Redes y de la Información, ENISA (por sus siglas en inglés), entró en funciones. Su principal objetivo es fortalecer la capacidad de la Unión Europea, los países miembros y las empresas para la reacción y gestión de problemas vinculados con la seguridad de las redes y de la información. Dicha entidad además de brindar asistencia y asesoramiento a la Comisión y a los países miembros también fomenta y facilita la cooperación entre entidades públicas y privadas.[58]

Poco a poco, la concientización sobre la seguridad y protección del ciberespacio se propagó por distintas entidades, por ejemplo en la reunión del 25 de julio de 2002 celebrada por la Organización para la Cooperación y el Desarrollo Económicos, OCDE, se recomendó la adopción directrices para la seguridad de sistemas y redes de información con objetivo de promover la cultura de la seguridad cibernética entre sus miembros. Con ello la OCDE promueve la cooperación e intercambio de información entre sus integrantes para el desarrollo y ejecución de políticas de seguridad, así como también de prácticas y

---

[56] Organización de Naciones Unidas. (Abril 12-19, 2010). 12º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal. (Nota 32 y 33). [En línea]. Disponible en:<http://www.unodc.org/documents/crime congress/12thCrimeCongress/Documents/A_CONF.213_9/V10503 85s.pdf>. (Consulta 11/11/13).

[57] Comisión de las Comunidades Europeas. (Marzo 30, 2009). *Proteger Europa de ciberataques e interrupciones a gran escala: aumentar la preparación, seguridad y resistencia*. EUR-LEX. [En línea]. Disponible en: <http://eurlex. europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:ES:HTML>. (Consulta 10/11/13).

[58] Europa, Síntesis de la Legislación de la UE. (Marzo 22, 2013). *Agencia Europea de Seguridad de las Redes y de la Información (ENISA)*. [En línea]. Disponible en: <http://europa.eu/legislation_summaries/information_society/internet/l24153_es.htm>. (Consulta 11/11/13).

procedimientos.[59] Por su parte el Foro de Cooperación Económica Asia-Pacifico, APEC (por sus siglas en inglés), a través del Grupo de Trabajo de Telecomunicaciones e Información celebró en 2002 un encuentro en Moscú con el fin de delinear la estrategia en ciberseguridad de de la APEC. La estrategia reconoce la importancia del convenio sobre ciberdelicuencia de la Unión Europea y orienta sus esfuerzos para cooperar con los objetivos de la Unión[60] y de la ONU —de acuerdo con la Resolución de la Asamblea General 55/63 "Lucha contra la utilización de la tecnología de la información con fines delictivos".[61]

Por parte de la Organización de Naciones Unidas, en abril de 2010, se celebró el 12º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal, en él reconoce las dificultades existentes para persecución de delitos informáticos y destaca la importancia de la cooperación entre naciones dada la trasnacionalidad de este tipo de infracciones, también plantea los conflictos derivados de la incompatibilidad legislativa entre los Estados, por lo que reconoce la necesidad de celebrar una convención internacional sobre el delito cibernético. En este congreso la ONU hace una revisión sobre la falta de normas nacionales e internacionales que persigan y castiguen el delito cibernético de forma efectiva y resalta la necesidad de preparar a las autoridades responsables de hacer frente a la amenaza emergente.[62] Sin embargo, en esta ocasión el papel de la ONU consistió únicamente en emitir recomendaciones y proponer la celebración de una convención internacional que desafortunadamente, hasta el momento, no se ha realizado. En octubre de 2004 la Unión Internacional de Telecomunicaciones, UIT, (organismo especializado de la ONU) realizó la Asamblea Mundial de Normalización de las Telecomunicaciones en la que, por medio de la resolución cincuenta, fortalece su papel en relación a la seguridad de las redes de comunicación e información. Lo más enriquecedor del evento fue el simposio celebrado días antes cuyo resultado es un reporte con observaciones,

---

[59] Organización para la Cooperación y el Desarrollo Económicos. (2006).*Directrices de la OCDE para la seguridad de sistemas y redes de información: Hacia una cultura de seguridad*. Ministerio de Administraciones Públicas y Secretaría General Técnica. España. [En línea].Disponible en: <http://www.oecd.org/internet/ieconomy/349 129 12.pdf>. (Consulta 11/11/13).

[60] Asia-Pacific Economic Cooperation. (Agosto 19-23, 2002). *APEC Cybersecurity strategy*. Telecommunications and Information Working Group. [En línea]. Disponible en: <http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN012298.pdf>. (Consulta 11/11/13).

[61] Asamblea General de Naciones Unidas. (Enero 22, 2001). *Resolución aprobada por la Asamblea General 55/63. Lucha contra la utilización de la tecnología de la información con fines delictivos*. Organización de Naciones Unidas. [En línea]. Disponible en: <http://www.unodc.org/pdf/crime/a_res_55/res5563s.pdf>. (Consulta 20/11/13).

[62] *Ídem.*

recomendaciones y propuestas relacionadas con la seguridad cibernética mundial y el papel de la cooperación internacional.[63] En septiembre de 2011, la ONU a través de la UIT dio un importante paso hacia la regulación y protección de las comunicaciones electrónicas internacionales con el establecimiento de la Alianza Internacional Multilateral contra las Ciberamenazas, IMPACT (por sus siglas en inglés), la cual reúne gobiernos, instituciones académicas y expertos en ámbito informático con el objetivo de mejorar las capacidades de comunidad internacional para hacer frente a las ciberamenazas.[64]

Respecto al continente Americano la Asamblea General de la Organización de Estados Americanos (OEA) aprobó en 2004 la Estrategia Interamericana Integral de Seguridad Cibernética con el fin de desarrollar la capacidad de defensa de los Estados miembros. Para lo cual se apoya en las experiencias del Comité Interamericano contra el Terrorismo (CICTE), la Comisión Interamericana de Telecomunicaciones (CITEL), y la Reunión de Ministros de Justicia o Ministros o Procuradores Generales de las Américas (REMJA). Como resultado, los Estados de la OEA se comprometen a fomentar la cultura de la seguridad informática y a tomar las medidas legislativas necesarias que procuren la confidencialidad y el buen uso de las tecnologías de la información y comunicación en sus territorios. La estrategia plantea la creación de una red hemisférica de Equipos de Respuesta a Incidentes de Seguridad en Computadoras (CSIRT) que funcione 24 horas al día, 7 días a la semana y que sea capaz de atender las necesidades de los países miembros en caso de un ataque informático. Adicionalmente cuenta con un grupo de expertos encargados de asesorar a los países miembros en la redacción y promulgación de leyes contra delitos cibernéticos, y de fomentar la cooperación entre autoridades.[65]

Para Lorenzo Valeri (2007), el establecimiento de un régimen internacional de seguridad cibernética requiere, además de esfuerzos individuales, que todos los integrantes del sistema

---

[63] Telecommunication Standardization Advisory Group. (Octubre 4, 2004).*Cybersecurity Symposium*. International Telecommunication Union. [En línea]. Disponible en: <http://www.itu.int/ITUT/worksem/cybersecurity/>. (Consulta 11/11/13).

[64] International Multilateral Partnership against Cyber Threats. *About the Global Cybersecurity Agenda. International Telecommunication Union.* [En línea]. Disponible en: <http://www.impactalliance.org/aboutus>/ITU IMPACT.html>. (Consulta 11/11/13).

[65] Organización de Estados Americanos. (Junio 8, 2004). *Estrategia de seguridad cibernética (RESOLUCION).* Comité Interamericano contra el Terrorismo. [En línea]. Disponible en: <http://www.oas.org/es/ssm/cyber/documents/Estrategia-seguridadciberneticaresolucion.pdf>. (Consulta 11/11/13).

internacional colaboren en el establecimiento de normas y leyes capaces de proteger la confidencialidad, integridad y disponibilidad de los sistemas de cibernéticos globales. De acuerdo con Valeri para ello será necesario superar intereses individuales a fin estructurar un régimen internacional que mitigue los efectos negativos del ciberdelito y asegure un entorno en en el que la sociedad internacional pueda desarrollarse y funcionar plenamente.

Al respecto la aportación más reciente proviene de la Organización del Tratado del Atlántico Atlántico Norte, OTAN, a través de la Declaración de la Cumbre de Chicago (2012) donde reconoce que la creciente sofisticación de los ataques informáticos demanda atención urgente por parte de la organización. Un año antes la OTAN adoptó nuevas políticas para la protección cibernética con el objetivo de responder de forma adecuada a las amenazas cibernéticas y proteger los sistemas informáticos de los países aliados, especialmente las infraestructuras críticas, también creó el plan de defensa inteligente, el cual busca desarrollar mecanismos y capacidades en los países miembros que les permitan alcanzar los objetivos de ciberseguridad planteados. También se creó el Centro de Excelencia de Ciberdefensa Cooperativa, CCDCOE (por sus siglas en inglés), ubicado en Tallin (Estonia) y acreditado por la OTAN en 2008. La CCDOE se encarga de realizar investigación y de capacitar personal para la defensa cibernética.[66]

En resumen, los esfuerzos en el plano internacional para la creación de una legislación que sancione los delitos informáticos son significativos; sin embargo, son llevados a cabo sólo a nivel regional o multilateral, en el ámbito internacional la ONU a través de la UIT básicamente se encarga de emitir recomendaciones.

Por otra parte, una tendencia clara en los instrumentos y mecanismos descritos anteriormente es la necesidad de promover la consciencia internacional con relación a la ciberseguridad, así como fomentar la cooperación entre naciones para facilitar el seguimiento de esta clase de delitos. La mayoría de las entidades internacionales invitan a la armonización de normas a fin de agilizar el intercambio de datos y la coordinación entre autoridades para sancionar el delito informático. Sin embargo, la efectividad de los mecanismos de cooperación internacional puede verse obstaculizada por múltiples factores, un ejemplo de esto es la

[66] North Atlantic Treaty Organization. (Octubre 22, 2013). *NATO and cyber defense*. [En línea]. Disponible en: <http://www.nato.int/cps/en/natolive/topics_78170.htm?>. (Consulta 20/11/13).

cancelación del Acuerdo de Transferencia de Datos bancarios (con EE.UU.) por parte de la Unión Europea, como respuesta a las operaciones de ciberespionaje de Estados Unidos.[67] esta situación resulta difícil pensar en una legislación internacional en materia de ciberseguridad, pues las operaciones de espionaje electrónico descubiertas en los últimos años enfrentan constantemente a múltiples naciones.

Para concluir, a pesar de las innegables debilidades del sistema jurídico internacional, es importante resaltar los esfuerzos realizados para la estructuración, actualización, y armonización de normas y mecanismos orientados a la seguridad cibernética. Así como, el establecimiento de organismos especializados en investigación, los cuales significan un paso importante para que la seguridad del ciberespacio y de los sistemas informáticos se convierta en un tópico esencial en el ámbito de la seguridad internacional.

1.2.4. Legislaciones en contra del ciberespionaje

Si la sociedad internacional posee un mayor de grado de consciencia sobre la seguridad cibernética se debe, en buena medida, a los ataques dirigidos a Estonia en 2007. En esa ocasión la comunidad internacional fue testigo de cómo un enemigo invisible derribó los sistemas informáticos de bancos, medios de comunicación y órganos estatales propagando el caos en el país. La vulnerabilidad de las estructuras criticas nacionales quedó demostrada con la declaración de ciberguerra a Estonia.

En la actualidad infraestructuras como la eléctrica, energética e hidráulica además de los sistemas financiero y comercial de prácticamente todas las naciones dependen de la estabilidad y buen funcionamiento de las redes cibernéticas; aunado a ello las bases de datos y los sistemas de comunicación de todas las entidades estatales dependen de Internet. El acontecimiento en Estonia significó para la sociedad mundial la necesidad de proteger el espacio en el circulan y se depositan la mayor cantidad de datos de la historia.

Sin embargo, pese a las lecciones aprendidas existen diversos países con legislaciones y mecanismos de ciberseguridad débiles. Quizá la ausencia de un ataque de esta naturaleza en su territorio les impida reconocer la importancia de medidas jurídicas en la materia. No

[67] Ulloa, Karina G. (Octubre 23, 2013). Eurocámara cancela datos bancarios para EE.UU. *Sexenio.* [En línea] Disponible en: <http://www.sexenio.com.mx/articulo.php?id=40146>. (Consulta 20/11/13).

obstante, un ataque cibernético afectaría tanto, y más, que una falla en el subministro eléctrico. En el último caso son evidentes los daños que causaría en sectores como el económico, financiero, de salud, y en el resto de los servicios proporcionados por el Estado; en el caso de ciberataque y específicamente de una operación de ciberespionaje los servicios pueden o no interrumpirse, pues generalmente los sistemas afectados continúan funcionando sin notar la intrusión. La gravedad de este tipo de acciones no debe subestimarse en el ámbito nacional, pues se trata de la sustracción de información sensible cuyo destino la mayoría de las ocasiones es desconocido.

Si en el ámbito internacional el marco jurídico todavía tiene muchos retos que enfrentar, en el caso de las legislaciones nacionales la situación se agrava. Son pocos los países que por iniciativa propia hayan impulsado el establecimiento de leyes contra el ciberdelito. Sin bien, el espionaje es una infracción tipificada en las leyes de seguridad nacional de múltiples Estados, la modalidad informática ha sido relegada.

El establecimiento de normas y leyes referentes a la seguridad informática se propagó de forma notable entre diversos países a comienzos de la década pasada, particularmente después que las TIC e Internet mostraron su enorme potencial como arma de guerra[68] (véase tabla 2). La mayoría de los marcos jurídicos de distintas naciones lograron desarrollarse gracias a que formaban parte de programas especiales impulsados por entidades regionales; por ejemplo, los países miembros de la Unión Europea están comprometidos a desarrollar y aplicar las disposiciones legales (y procedimientos) necesarios para proteger e impulsar el buen funcionamiento de Internet, específicamente medidas relacionadas con la privacidad en la red, manipulación de datos, ataques contra la integridad de sistemas informáticos, acceso o intercepción ilícita, atentados contra la propiedad intelectual, etc. debido a que forman parte del Convenio de Budapest. Lo mismo ocurre con los Estados miembros de la Organización de Estados Americanos a través de la "Estrategia Interamericana Integral de Seguridad Cibernética" y con los miembros del Foro de Cooperación Económica Asia-Pacífico, APEC (por sus siglas en inglés), a través de Resolución de la Asamblea General 55/63 de la Organización de Naciones Unidas.

[68] Las aportaciones legales más notables se desarrollaron después del acontecimiento en Estonia o como consecuencia del descubrimiento de ataques cibernéticos en diversos Estados.

Tabla 2. Legislaciones para la seguridad cibernética

País	Medidas adoptadas
Alemania	En Febrero de 2011 lanzó el Programa de Seguridad Cibernética y en abril, de ese mismo año, el Ministerio de Interior puso en funciones el Centro Nacional de Ciberdefensa.
Australia	Creó en 2010 el Centro de Operaciones Cibernéticas encargado de coordinar acciones estatales ante incidentes ocurridos en el ciberespacio.
Canadá	El departamento de Seguridad Pública puso en funcionamiento el Centro Canadiense de Respuesta a Incidentes Cibernéticos (CCIR) y en octubre de 2010 adoptó la Estrategia Canadiense de Seguridad Cibernética.
Corea del Sur	En 2009 anunció la creación de un Comando de Defensa Cibernética subordinada al Ministerio de Inteligencia y Defensa. En 2012 se lanzó un nuevo Comando de Defensa Cibernética que, según aproximaciones, emplearía entre 400 y 500 ciberguardianes.
Estados Unidos	Centro de Ciber-Comando Unificado que depende de: la Agencia de Seguridad Nacional; de la División Nacional de Seguridad Cibernética, la US-CERT; del Equipo de Emergencias Informáticas de Estados Unidos y la Oficina de Seguridad Cibernética de la Casa Blanca. En mayo de 2011 adoptó la Estrategia Internacional para el Ciberespacio.
Estonia	En 2008 junto a países de Europa, la OTAN y Estados Unidos crearon el Centro Internacional de Análisis de Ciberamenazas, y adoptó una Estrategia de Seguridad Cibernética.
Francia	Creó la Agencia de Seguridad para las Redes e Información (ANSSI) que vigila sistemas informáticos tanto públicos como privados. En 2011 adoptó la Estrategia para Defensa y Seguridad de los sistemas informáticos.
México	La Comisión Nacional de Seguridad por medio del Centro Nacional de Respuesta a Incidentes Cibernéticos (CERT-MX) realiza patrullajes en la red pública de Internet con el fin de identificar alguna actividad cibernética maliciosa.
Reino Unido	En junio de 2009 publicó la Estrategia de Seguridad Cibernética que estipula la creación de la Oficina de Ciberseguridad (OCS) y del Cetro de Operaciones para la Seguridad Cibernética (CSOC) para monitorear y responder a cualquier tipo de actividad cibernética. Adicionalmente cuenta con el Centro para la Seguridad de las Tecnologías de Información (CSIT) en Irlanda del Norte.
Rusia	La Doctrina de Seguridad Informática fue aprobada por Vladimir Putin en el año 2000.

Fuente: Elaboración propia con datos obtenidos de Conpes. *Lineamientos de Política para Ciberseguridad y Ciberdefensa*. 2011; Richard Stiennon. *Surviving Cyberwar*. 2010, y SEGOB. *Denuncia Delitos Cibernéticos*. 2013.

En conclusión, la ausencia de un régimen internacional en materia de seguridad informática se debe a que se ha desarrollado un "régimen internacional de letra muerta", de acuerdo con Lorenzo Valeri (2007) es difícil pensar que la sociedad internacional pueda adoptar una normatividad general de seguridad informática cuando ésta ha sido impulsada por actividades delictivas provenientes de distintos Estados. Los regímenes de letra muerta se caracterizan por la poca disposición de las partes para reconocer sus principios, normas, leyes y procesos de toma de decisiones, en pocas palabras: ninguno de los participantes siente la obligación de respetar el régimen. Esta situación es consecuencia de un imperante clima de desconfianza entre las partes. Por lo que en la actualidad los esfuerzos orientados a la seguridad cibernética básicamente dependen del trabajo que desempeñe cada nación o bloque regional.

Capítulo 2. Las Relaciones Internacionales, la diplomacia electrónica y la ciberguerra

El presente capítulo analiza la importancia de las comunicaciones en la escena así como las transformaciones generadas por la revolución tecnológica; específicamente se examinan los efectos producidos en la diplomacia y en la percepción general de los conflictos interestatales. A continuación, considerando que tanto el espionaje como las filtraciones forman parte intrínseca de la interacción entre naciones se profundiza en las implicaciones generadas por el uso de nuevas tecnologías en dichas actividades. Por último se estudia el papel que desempeña la llamada Sociedad de la información en la práctica diplomática contemporánea, y la aparente redistribución del poder entre diversos actores del escenario mundial.

El estudio de las Relaciones Internaciones es particularmente complejo, ya que el principal elemento en ellas (el Estado) se encuentra en permanente proceso de transformación, en suma existe una gran variedad de factores que inciden de forma directa o indirecta en su comportamiento. Sin embargo, a lo largo del tiempo cientos de expertos se han esforzado por aprehender, analizar y compartir la imagen más fiel de la realidad mundial.

A grandes rasgos, la comunidad internacional se enfila hacia el nuevo siglo en medio de una crisis económica que pareciera demostrar el lado obscuro de la globalización; persistentes protestas sociales que reflejan la incansable lucha del hombre por mejores niveles de subsistencia; viejos y nuevos conflictos en lugares como Medio Oriente que comprueban que pueden evolucionar a mayor velocidad que los mecanismos encargados de remediarlos; por último los avances científico-tecnológicos que han transformado totalmente el panorama social y político de múltiples naciones. Estas circunstancias promueven el desarrollo de nuevos análisis que ayudados de los modelos tradicionales permitan exponer los beneficios que la disciplina de las Relaciones Internacionales puede aportarle al mundo.

En este sentido la aplicación y desarrollo de tecnologías de la información y la comunicación han logrado alterar la naturaleza del sistema mundial; sin embargo, no se trata de un fenómeno reciente, pues desde siempre las vías de conexión han ocupado un lugar especial en el estudio de las Relaciones Internacionales, al respecto Celestino del Arenal

(1985) sostiene que son capaces de determinar la configuración y el comportamiento de la dinámica mundial. Ante ello los avances tecnológicos experimentados en los últimos años han impulsado la creación de redes trasnacionales multidireccionales, lo que ha provocado la reconfiguración de la escena interestatal, actualmente caracterizada por un incremento del flujo de información y la incorporación de nuevos actores.

Esta tendencia ha sido examinada a través la teoría de las comunicaciones —cuyo principal representante es Karl W. Duscht— y la cual sostiene que las TIC ejercen influencia en la política (condicionando su comportamiento) y en la evolución de la sociedad. Al respecto, en el modelo de esta teoría propuesto Tooze (1987) se analiza la transformación de las comunicaciones internacionales en términos complejos y multidimensionales, desde este enfoque los mensajes e interconexiones acaecidas en el ámbito mundial son elementos que permiten comprender el sistema.

De la misma forma para J. W. Burton (1965) las comunicaciones conforman y amoldan la estructura internacional. Especialmente en su obra *International Relations. A General Theory* advierte una disminución en el papel de la fuerza y el poder, al tiempo en el que los procesos de toma de decisiones adquieren mayor terreno, de esta forma la percepción de los países respecto a la política exterior de otros adquiere importancia; aunado a ello tanto los cambios internos como la capacidad de adaptarse a éstos se vuelve trascendente entre los miembros de la comunidad. En síntesis las rutas y vías de comunicación construyen el sistema internacional y determinan su comportamiento. Por tal motivo, la evolución de las TIC ha impulsado la trasformación de dicho escenario a lo largo de diversas etapas. Recientemente la liberalización de información y la expansión global de redes de interacción ha provocado la evolución del comportamiento particular y colectivo de los individuos, y de las propias naciones.

Por otra parte, la diplomacia entendida como un instrumento para promover el interés nacional, encausado en la política exterior, constituye la vía principal de conexión de un país con el resto del mundo, y por ende, el elemento que forma directa ha experimentado la evolución del ecosistema internacional.

De acuerdo con Joseph Nye Jr. (2003) las comunicaciones han transformado el concepto de poder y soberanía de los Estados, la red como espacio intangible ha desafiado las formas

convencionales de control, provocando que algunas naciones establezcan todas las medidas posibles para restringir el uso de las TIC. En adición con la llamada "democratización de la información" el peso de la opinión pública en la estructuración de la política exterior ha incrementado, modificando también el ejercicio diplomático tradicional. Según Rafael Rubio (2011) esta alteración se ve reflejada en la preferencia del poder blando sobre el poder duro, y ha provocado que las naciones no sólo se preocupen por mejorar las relaciones con otros Estados sino también con otros actores, ya que la opinión pública (nacional e internacional), las ONG y otros agentes no estatales están siendo incluidos a una nueva práctica diplomática.

Ante este nuevo escenario, la diplomacia ha modificado, tanto sus objetivos como sus métodos. Si adoptamos la lógica de Nye, aquellas naciones que se resistan a transformar dichos factores (prácticas y objetivos) y a considerar a la comunicación como una pieza central en el engranaje internacional serán incapaces de funcionar adecuadamente en el escenario contemporáneo. Esta nueva diplomacia es concebida por Melgar (2010) como un conjunto de instituciones y estrategias ideales para la proyección de la imagen de un país en la opinión pública internacional.

En otras palabras, la diplomacia se traslada hacia un foro abierto, caracterizado por el establecimiento de múltiples canales interactivos donde la opinión de la mayoría tiene un papel preponderante. No se trata del vencimiento del modelo tradicional, sino de perfeccionar su práctica. La Era tecnológica llama a replantear los viejos mecanismos donde la diplomacia aparecía como un elemento restringido y casi secreto, y hace una invitación para privilegiar el diálogo tanto a nivel interno (en la estructuración de las estrategias de política exterior) como a nivel internacional (al incluir a nuevos actores).

Bajo esta misma línea surge el concepto de diplomacia electrónica o *e-diplomacy*, que a su vez proviene de la tendencia internacional a sincronizar viejas prácticas (*e-government*, *e-commerce*, *e-democracy*, etc.) con la evolución de las TIC, buscando eficiencia y aprovechando al máximo el potencial comunicativo. De acuerdo con Nicholas Harkiolakis (*s.f.*) la diplomacia ha llegado a las masas, pero también ha beneficiado a los gobiernos y a los representantes oficiales, permitiéndoles acceder a información importante a una

velocidad casi inmediata; sin embargo, también aumentan las amenazas y vulnerabilidades, donde el espionaje y las filtraciones aparecen como elementos referentes de una ciberguerra.

Harkiolakis también advierte mayor influencia de las ONG que al repercutir de forma directa en las masas modifican la tarea diplomática contemporánea. Estas y otras entidades de la sociedad civil explotan al máximo las ventajas tecnológicas estableciendo comunidades virtuales con la firme intención de consolidarse como actores importantes en la arena internacional. En este sentido la red como herramienta organizativa facilita la formación y coordinación de movimientos nacionales e internacionales capaces de influir en la opinión de la pública. Harkiolakis sugiere que el entorno internacional está determinado por las TIC, quienes también han redefinido la naturaleza diplomática, convirtiéndola en un modelo flexible, menos jerárquico y con mayor número de participantes.

De acuerdo con Eugene N. Nweke (2012), la *e-diplomacy* debe servir como herramienta para que los Estados procuren la participación ciudadana, pues además de promover la comunicación facilita el intercambio de conocimientos; sin embargo señala que existen tanto individuos como naciones que están siendo restringidas de sus beneficios a causa de la llamada "brecha digital", y afirma que el rumbo de la política exterior y el de la diplomacia están siendo condicionados, limitados e influenciados por actores no estatales que han obtenido mayor proyección gracias a las aplicaciones tecnológicas. Según Nweke la liberalización del conocimiento ha provocado que el Estado pierda el monopolio de la información. En este aspecto, el surgimiento de filtraciones masivas confirma el libre flujo de datos y también desmitifica la práctica diplomática.

Dado que las comunicaciones electrónicas se están convirtiendo en el principal elemento de comunicación para los Estados tanto a nivel interno como externo se han generado nuevos desafíos para la seguridad. En este punto surge el concepto de Ciberguerra, que ya ha sido analizado por diversos Centros e instituciones especializadas en seguridad, y por académicos como John Arquilla y David Ronfeldt.[69] Concretamente el término se refiere al uso de Internet o de software maliciosos por parte de un Estado (o grupo de Estados) para atacar la estructura

[69] Ver John Arquilla y David Ronfeldt, *Redes y guerras en red: el futuro de Terror, Crimen y Militancia*. RAND Corporation, 2001, e *In Athena's Camp: Preparing for Conflict in the Information Age*. RAND Corporation, 1997.

funcional (o decisional) de uno o más países.[70] Desde 1996 John Deutch, entonces Director de la Agencia Central de Inteligencia (de Estados Unidos), señaló que los alcances de las actividades cibernéticas hostiles provenientes de determinados Estados eran señal de que un "Pearl Harbor Electrónico" estaba cerca.[71] Quizá en esos momentos dada la limitada expansión de Internet la declaración de Deutch fue considerada un tanto alarmista, pero en 2007 los ataques contra Estonia confirmaron el potencial destructivo del armamento cibernético que en ese entonces fue utilizado en contra de sistemas nacionales e infraestructura crítica. Después del incidente diversas organizaciones mundiales solicitaron que la seguridad electrónica se convirtiera en una prioridad dentro del sistema internacional.[72]

2.1. Espionaje y filtraciones diplomáticas en la era tecnológica

Si la información constituye en un elemento de poder, tanto para la sociedad como para los Estados, su control y manipulación representa una importante herramienta política. Por esta razón el espionaje y las filtraciones son prácticas que han estado presentes en las historia de las naciones. A través del tiempo los casos de espionaje diplomático han impulsado la optimización de los mecanismos de comunicación, y más aún cuando los datos que circulan por dichas vías se relacionan con temas tan sensibles como conflictos bélicos y negociaciones; sin embargo, con la revolución tecnológica los métodos para interceptar, robar o filtrar información se han amplificado. De esta forma surge un dilema en donde la apertura aparece como requisito para subsistir en el escenario internacional contemporáneo, pero también aparece la necesidad de proteger las comunicaciones ante herramientas cibernéticas tan complejas y efectivas capaces de sorprender a cualquiera.

Particularmente a principios de este siglo comenzaron a efectuarse operaciones de ciberespionaje diplomático en donde la sofisticación de los métodos utilizados evidenció que si bien las prácticas diplomáticas intentan evolucionar a la par de las TIC, los mecanismos

---

[70] Centro Superior de Estudios de la Defensa Nacional. (Marzo, 2012). Los Ámbitos No Terrestres en la Guerra Futura: Espacio. Monografías del CESEDEN, no. 128. [En línea]. Disponible en: <http://www.defensa.gob.es/ceseden/Galerias/destacados/publicaciones/monografias/ficheros/128_LOS_AMBITOS_NO_TERRESTRES_EN_LA_GUERRA_FUTURA_ESPACIO.PDF>. (Consulta 03/02/2014).

[71] CSIS Global Organized Crime Project, Center for Strategic and International Studies. (1998). *Cybercrime--Cyberterrorism-- Cyberwarfare--: Averting an Electronic Waterloo*. Washington, D.C.: CSIS Press.

[72] Stiennon, Richard. (2010). *Surviving Cyberwar*. Reino Unido: Government Institutes.

de defensa han quedado relegados. El desarrollo de herramientas especiales para irrumpir las comunicaciones oficiales demuestra que mientras el mundo continuaba sorprendiéndose con los los pasos de la innovación tecnológica organizaciones anónimas estaban desarrollando y ejecutando operaciones masivas de espionaje cibernético.

Por otra parte, el surgimiento de filtraciones diplomáticas le demuestra al mundo la verdadera naturaleza de la interacción internacional, y colocan a los Estados ante la disyuntiva de elegir qué datos deben compartirse con la sociedad del conocimiento, y cuáles deben ser protegidos en el marco de la diplomacia pública contemporánea. Sin embargo, la extensión y capacidad de las actividades ilícitas en Internet han llamado la atención de diversas naciones quienes abogan por controlar la red de redes ante la aparición de modalidades como el terrorismo y el espionaje electrónico a fin de combatir la "ciberanarquía", de acuerdo con Goldsmith (1998). No obstante, en esta como en muchas otras situaciones se puede caer en medidas extremas, en este sentido Kingsmith (2013) sostiene que la reacción de las naciones dominantes ante las filtraciones diplomáticas de 2010 confirma una tendencia internacional hacia la macrosecuritización digital.[73]

Será difícil que los actores del escenario mundial puedan encontrar un equilibrio respecto al control de la web. Empero, es un hecho que la autopista virtual se ha convertido en un medio de comunicación diplomática (sino es que en el principal), por ello es necesario establecer las medidas técnicas y jurídicas necesarias para protegerla. En este sentido también es evidente que en adelante las naciones abogaran por mejores mecanismos de protección de sistemas y de bases de datos tanto dentro de su territorio como en el exterior. Los casos de ciberespionaje electrónico revelados en los últimos años respaldan la aseveración de Bendrath (*et. al.* 2007) acerca de que la legitimización de medidas extremas tiene mayor probabilidad de efectuarse cuando se percibe un antagonista que intencionalmente desea hacer daño. Sin embargo, el establecimiento de medidas preventivas debe efectuarse cuando se localizan las deficiencias de

[73] Que a su vez hace referencia a la teoría de la securitización impulsada por la Escuela de Copenhague, la cual consiste en el posicionamiento (a través del discurso) de una situación o actor determinado como una amenaza a la supervivencia de un objeto referente; una vez que el posicionamiento se ha legitimado por un sector relevante se admite el establecimiento de medidas de emergencia fuera de los canales políticos tradicionales. Fuente: McDonald (2008).

un sistema a través del análisis y el estudio, y no frente a la precepción de una amenaza inminente, pues en este escenario el tiempo dedicado a un consenso es mínimo.

2.2. La sociedad de la información y la nueva diplomacia

El término "Sociedad de la información" fue utilizado por primera vez por Machlup en ese entonces se usó para referirse al considerable número de personas que utilizaban los medios de comunicación. A través del tiempo algunos teóricos han recurrido a diversas expresiones para referirse a los cambios sociales generados por la evolución de las vías de comunicación.[74] Sin embargo, en 1975 la Organización para la Cooperación y el Desarrollo Económicos (OCDE) retomó el concepto (Sociedad de la información) y en adelante se convirtió en un elemento recurrente en los discursos de entidades internacionales.[75]

En síntesis, la Sociedad de la información representa un espacio abierto, dinámico y global donde el conjunto de relaciones sociales se apoya y realiza a través de la información y de las nuevas tecnologías.[76]

A la postre, Matterlart (2002) percibió que dicha transformación había generado una nueva etapa de las prácticas diplomáticas; en este sentido señala que somos testigos de una nueva forma de utilizar información estratégica con el fin de provocar determinadas reacciones en el entorno internacional. De acuerdo con Matterlat dentro de esta nueva mecánica la democracia aparece como única garantía de un mundo seguro, discurso que ha sido utilizado con frecuencia para legitimar las acciones de la política exterior de determinadas naciones. En pocas palabras, para Matterlart la revolución tecnológica otorga un nuevo impulso al uso del *softpower* con el objetivo de influenciar la opinión pública internacional.

---

[74] Comisión Económica para América Latina y el Caribe. (2008). *La sociedad de la información en América Latina y el Caribe: Desarrollo de las tecnologías y tecnologías para el desarrollo*. División de Desarrollo Productivo y Empresarial, y Programa Sociedad de la Información. [En línea]. Disponible en: <http://www.oei.es/tic/cepal.pd>. (Consulta 10/02/2014).

[75] Matterlart, Armand. (2002). *Historia de la Sociedad de la Información*. España: Paidós Ibérica.

[76] Garduño Vera, Roberto. (2004). "La Sociedad de la Información en México frente al uso de Internet". *Revista Digital Universitaria*, vol. 5, no. 8, pp. 2-13. [En línea]. Disponible en: <http://www.revista.unam.mx/vol.5/num8/art50/sep_art50.pdf>. (Consulta 10/02/2014).

Por otra parte, la convergencia de la Sociedad de la información y la nueva diplomacia, de acuerdo con Henrikson (2013), ha provocado mayor apertura de información y la expansión de canales de expresión que suponen la desaparición de la diplomacia como intermediaria entre el Estado y la sociedad, desde esta perspectiva la diplomacia pasa a ser un espectador. En el pasado los representantes oficiales manejaban una gran cantidad de información de manera casi exclusiva que se encargaban de transmitir a sus respectivos países. Con el arribo de la Era tecnológica tanto las ofertas como las fuentes de información inundaron el ciberespacio y otorgaron a la ciudadanía nuevos canales de interacción con sus representantes; en suma organizaciones internacionales, ONG y asociaciones civiles adquirieron mayor presencia en la escena internacional siendo capaces de influenciar en la negociación entre países. Ante dicho escenario la tarea diplomática se ha vuelto compleja, hoy día debe incorporar nuevos participantes, y adoptar nuevas vías de conexión.

De esta forma las capacidades adquiridas por los nuevos participantes transforman la identidad de los Estados-nación como protagonistas de las relaciones internacionales. De acuerdo con Lozano Bartolozzi (1999), la diplomacia ha experimentado diversas fases de evolución a lo largo de la historia pasando de cumplir una función meramente informativa (donde aparecía como actor principal) a ser parte de una estructura compleja (donde participantes como los medios de comunicación y la opinión pública internacional atenuaron su protagonismo). Bartolozzi señala que el surgimiento de la Sociedad de la información ha impulsado el desarrollo de un modelo diplomático abierto, y que en los últimos años ha incorporado a la práctica el uso de herramientas tecnológicas, extendiendo su presencia en el ciberespacio.

Al respecto Castro de Ruano (2000) declara que esta nueva forma de diplomacia supera los canales y métodos convencionales que eran utilizados por los mecanismos tradicionales, y que la diplomacia aparece como un instrumento para proyectar una imagen internacional favorable a los intereses internos, como consecuencia la política exterior de las naciones se ha vuelto más accesible. Para Castro de Ruano el surgimiento de una nueva práctica diplomática no hubiera sido posible sin la convergencia de tres fenómenos: la generalización de la democracia; la revolución telemática y la aparición de la Sociedad de la información, y la globalización.

Empero, la práctica diplomática aún experimenta transformaciones, en años recientes el rol de organizaciones internacionales, ONG y de la sociedad internacional en general ha sido más activo, ello demanda el establecimiento de mecanismos diplomáticos de interacción eficaces; si bien hoy día la actividad diplomática puede ser consultada en la red a través de portales oficiales y de agencias de noticias, la Sociedad de la información exige el establecimiento de foros sociales. Al respecto durante manifestaciones en Medio Oriente (pertenecientes a la llamada Primavera árabe) la diplomacia tradicional enfrentó grandes desafíos, pues la sociedad internacional esperaba la oportuna respuesta de entidades como la Organización de Naciones Unidas, y demandaba el establecimiento de la democracia y la garantía del respeto a los derechos humanos durante la transición. Recientemente ante la negociación de posibles soluciones para el conflicto en Siria la comunidad mundial rechazó la propuesta de una intervención directa, estos casos confirman que la opinión pública internacional es capaz de determinar el rumbo de la diplomacia, ya que se ha incorporado eficazmente en la dinámica mundial a través de las nuevas tecnologías.

2.3. El Estado, el poder y la innovación tecnológica

La propuesta y desarrollo del paradigma digital en las relaciones internacionales se caracteriza por una aparente redistribución del poder, así como por la incorporación de nuevos actores.

En este sentido, Darin Barley (2003) propone el surgimiento de una *ciberesfera pública* que de acuerdo con Habermas (2001), es capaz de construir un debate critico-racional sobre cuestiones de interés general, mediante este mecanismo la opinión pública es capaz de legitimar el comportamiento de quienes ocupan el poder. Para Barley las nuevas tecnologías han contribuido a la estructuración de una esfera pública democrática donde la opinión de la mayoría tiene más importancia. Sin embargo, de acuerdo con Barley el uso cada vez más frecuente de las nuevas tecnologías ha llevado a los ciudadanos a un proceso de individualización —en el sentido en que los aleja de los procesos tradicionales de convivencia y los encierra en sí mismos— de esta forma la tolerancia hacia otras concepciones de la realidad puede verse afectada, en este punto surge lo que Robert Putman (2000) ha definido como "ciberbalcanización".

Por otra parte, Habermas (2001) plantea que la participación actual de la sociedad internacional a través de las nuevas tecnologías es bajo la modalidad de consumidor y no como miembro activo, ya que por lo generalel uso de las TIC tiene como objetivo comerciar bienes o servicios, o bien recibir información, desde esta perspectiva la sociedad contemporánea no se caracteriza por ser un elemento crítico del sistema mundial.

Bajo esta misma línea, Pippa Norris (1999) sostiene que las nuevas tecnologías no han estimulado el surgimiento de nuevos actores en la escena mundial, sino que han otorgado mejores instrumentos de participación política a la convencional minoría participativa. En adición Barney señala que la esfera cibernética se ha visto afectada por la presencia inminente de agentes de consumo y de entretenimiento, que de acuerdo con Habermas resultan corrosivos para el buen funcionamiento de la esfera pública.

Al respecto Dwayne Winseck (2001) señala que los grandes conglomerados industriales están ocupando la *World Wide Web* como un instrumento para incrementar sus beneficios, y la han transformado en una especie de extensión para promover y procurar sus intereses en la comunidad digital mediante el establecimiento de normas para la regulación de las redes (tanto de contenidos como de prácticas), promoviendo una técnica horizontal y vertical capaz de controlar el ciberespacio, con ello la descentralización y libertad características de la nueva esfera pública corren peligro de desaparecer. Desde esta perspectiva la red aparece como instrumento de dominio económico y político, en lugar de un nuevo espacio de dialogo y democracia.

Existen diversos análisis sobre la forma en la que las TIC han transformado la dinámica social y política. Al respecto Christopher Wilson (2013) ha concentrado sus esfuerzos en analizar la transformación de los modelos de cooperación y su repercusión en la distribución del poder.

Para Wilson las nuevas tecnologías han transformado el ecosistema social y político, por lo que las formas tradicionales de gobernanza pueden resultar obsoletas; de ser así señala que es necesario estructurar un modelo capaz de reemplazar al existente. Desde esta perspectiva la opinión pública es uno de los elementos que colabora a la estructuración de nuevas formas de gobernanza, sin embargo existen otros agentes que también participan en dicha tarea (véase

figura 1). En adición cada uno de estos elementos está siendo alterado por la adopción de nuevas tecnologías.

Figura 1. Elementos que asisten a la trasformación del modelo de gobernanza

Fuente: Wilson, Christopher. (2013). "Internet Will Make Governments Unrecognizable by Today's Standards: From Leadership to Stewardship and Collaboration." Universidad de Ottawa. Montreal p. 3

Si bien Wilson admite que el Estado sigue siendo la autoridad central y el único encargado de solucionar conflictos de diversas clases (como económicos, políticos, sociales, etc.), también sostiene que se enfrenta a nuevas circunstancias, entre ellas: 1) incremento en la complejidad de sus funciones; 2) la liquidez estatal; 3) la disminución del estado de bienestar; 4) la necesidad de nuevas formas de gobierno, y 5) el desafío que representa Internet.

En cuanto a los cambios en la sociedad McLuhan (1996) señala que la aldea global está caracterizada por el surgimiento de una interdependencia electrónica, donde los modelos sociales se trasladaran de mecanismos individuales a la creación de una identidad colectiva que promueve mejores lazos de cooperación; sin embargo, esta forma de convivencia tambien genera nuevos conflictos.

En sintesis, la adopción de innovaciones tecnologicas no sólo incrementa la interacción interestatal tambien la transforma.

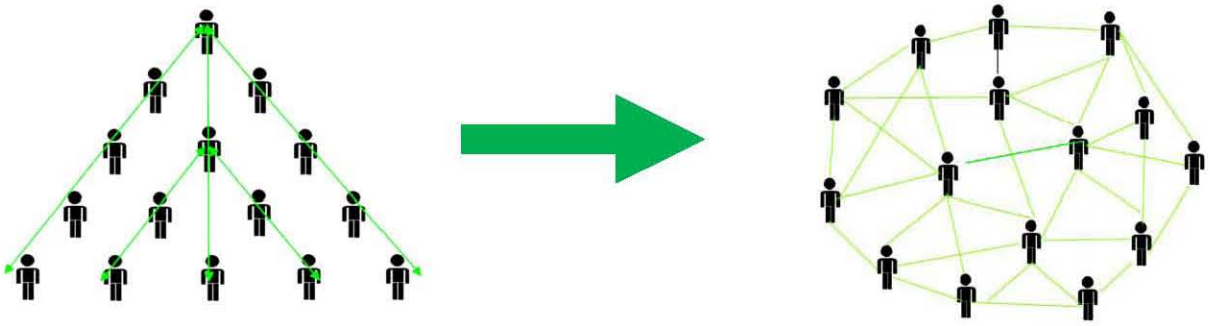
Respecto al papel del Estado Wilson advierte una perdida en el control de la información que se ve reflejada en la demanda de mayor transparencia en los organismos nacionales e internacionales. Dicha capacidad de control se ha visto afectada por la aparición de fugas de información —por parte de miembros de la burocracia, hackers o por deficiencias en los sistemas electrónicos.

En general, tanto las estructuras como los funcionarios estatales han perdido privacidad y tambien la capacidad de mantener en secreto actividades ilicitas o poco eticas. En este aspecto los representates de gobierno, funcionarios, politicos e instituciones deben considerar que cada una de sus decisiones será examinada por un número importante de personas, por lo que deberán mejorar los mecanismos de transparencia y rendición de cuentas si esperan ser legitimados y apoyados por la sociedad.

Wilson tambien señala que el concepto de liderazgo ha sido transformado. En adición, la aceptación de un lider político por parte de la sociedad no sólo depende de elementos como la ética o la efectividad sino también de los modelos de acción implementados en busca del bienestar común. En este sentido las jerarquias han sido desplazadas por formas de colaboración más partipativas y menos autoritarias.

Dado que la diversidad de problemas que deben enfrentar los Estados se ha multiplicado también los elementos necesarios para solucionarlos han aumentado. Cada vez más organismos son incluidos en la dinámica estatal con el objetivo de colaborar al beneficio social, es por esta razón que el liderazgo ha perdido importancia y se ha establecido un modelo más amplio de colaboración social. Esta supuesta distribución de poder a llevado a que academicos como Mearian (2013) consideren que la proxima revolución en América no será tecnológica sino social. En resumen para Wilson el modelo piramidal ha quedado atrás para ser reemplazado por un esquema en red (véase figura 2).

Figura 2.Transformación de los mecanismos de coordinación y acción social



Fuente: Wilson, Christopher. (2013). "Internet Will Make Governments Unrecognizable by Today's Standards: From Leadership to Stewardship and Collaboration." Universidad de Ottawa. Montreal, pp. 28 y 33.

Desde otra perspectiva Castro de Ruano establece dos discursos respecto al impacto de las TIC en el escenario mundial: el integrado y el crítico.

En el primero se exaltan los beneficios de las nuevas tecnologías y se prevé una adopción masiva que indudablemente repercutirá en la conformación del sistema mundial, esta tendencia ya había sido anunciada por Karl Deutch (1981) en forma de una "aculturación masiva" caracterizada por la pérdida gradual de rasgos idiosincráticos locales a favor de una inculturación general, y de nuevos valores generales o globales propios de la nueva civilización tecnológica. Desde esta perspectiva las nuevas tecnologías alientan el surgimiento de una sociedad más libre y democrática que facilitará la redefinición de las relaciones Norte/Sur; este sistema se caracteriza por la ausencia de una jerarquía rígida y de un sólo centro de poder. Aunque para Matterlart (1998) esta interpretación es un tanto exagerada, pues en periodos anteriores de la historia se exaltaron también los beneficiosos de otros medios como las redes marítimas y ferroviarias. Empero para Castro de Ruano las comunicaciones hoy día son concebidas como herramientas para promover la comunidad y la cohesión, y también son vistas como garantía de la paz social.

Del lado de discurso crítico las TIC no son libertadoras sino instrumentos de dominación y opresión, pues contribuyen a la desinformación y al aumento de las desigualdades sociales; en resumen las nuevas comunicaciones no hacen más que beneficiar al capitalismo mundial. Desde esta óptica el dominio del Norte sobre el Sur es persistente, y el desequilibrio de oportunidades y circunstancias es constante; por lo que las comunicaciones

sirven como herramientas para legitimar, defender y difundir determinadas representaciones y configuraciones de la realidad global. Desde esta óptica el modelo centro-periferia no ha expirado.

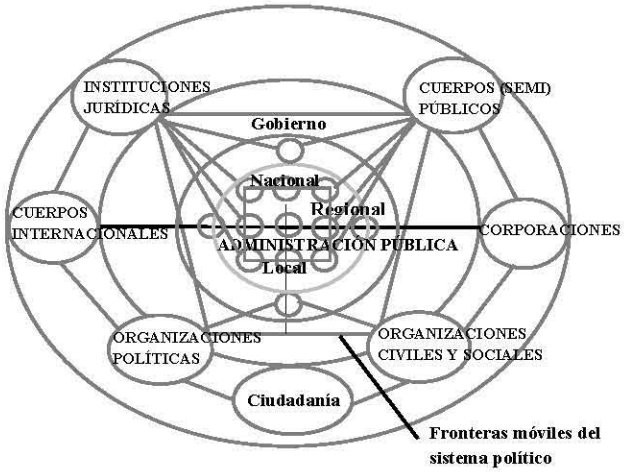
De Ruano también identifica una asimetría en el nuevo orden internacional que es más compleja que la diferencia entre norte y el sur o centro y periferia. Bajo esta misma línea según Petrella (1993) el mundo es asimétricamente interdependiente, es decir tanto el Norte como el Sur son cada vez más heterogéneos. De acuerdo con Castells (1997) se trata de una nueva geometría del poder.

Respecto a este punto Dunn (2007) sostiene que en los últimos años se ha dado una transformación en la estructura del poder, ya que el desarrollo de las TIC ha provocado una configuración compleja más allá de los tres pilares tradicionales.[77] De esta forma la redistribución del poder producirá dos consecuencias: 1) el colapso del pilar económico dado el surgimiento de mercados electrónicos globales y la internacionalización de las empresas tradicionales que generarán conflicto en las políticas orientadas al control del mercado; 2) la concepción de que las nuevas tecnologías generarán el surgimiento de nuevos actores que desafiarán la posición de los Estados como protagonistas del sistema mundial. Dunn prevé que en el futuro del sistema internacional se experimentará una bifurcación en las estructuras globales que se caracterizará por el surgimiento subsistemas multicéntricos.

Bajo esta misma línea, Kennet Hacker y Jan van Dijk (2000) proponen un modelo internacional dinámico en donde la interacción con otros participantes será importante, en esta propuesta se toma en cuenta la división convencional de poderes, y la distinción entre Estado y sociedad; se trata de un modelo neutral, descriptivo y explicativo. Desde este punto de vista la política y el poder no son consideradas como propiedades de individuos o de colectividades sino características de una interacción dinámica (véase figura 3).

[77] De acuerdo con Dunn los tres pilares tradicionales del poder son la fuerza económica, militar y política.

Figura 3. Modelo sistémico-dinámico de la estructura internacional



Fuente: Hacker, Kenneth y Jon Van Dijk. (2000). Digital Democracy. Issues of Theory and Practice. SAGE Publications, Reino Unido.

En síntesis, los cambios en la dinámica internacional son evidentes, ya sea con el surgimiento de nuevos actores o con el empoderamiento de viejos participantes, el incremento en el flujo de información y el establecimiento de nuevas redes y vías de conexión han creado una estructura compleja en donde la opinión pública resurge como factor importante. En este sentido el Estado ha perdido cierto grado de protagonismo, sin embargo conserva autoridad en cuestiones como seguridad, política y economía. Esto no quiere decir que será reemplazado por otros elementos sino que deberá interactuar con otros participantes a través de nuevos medios. En pocas palabras sistema mundial se está volviendo multipolar, por lo que la estabilidad del mismo dependerá de la cooperación y flexibilidad de todos los actores.

Capítulo 3. *WikiLeaks* y la diplomacia

En este capítulo se abordarán el funcionamiento, la historia y las influencias de la organización *WikiLeaks*. A continuación, se presenta un análisis sobre la publicación de filtraciones (significado y antecedentes), la reacción generada en la esfera internacional y un estudio sobre sus repercusiones en el ámbito diplomático. Desde una perspectiva general se abordan los retos que plantea el uso de las TIC para el ejercicio periodístico convencional y la relación entre las nuevas tecnologías y los movimientos sociales. En último lugar se analizarán las consecuencias políticas generadas por *WikiLeaks*, en vistas de una regulación para el ciberespacio.

Antes de 2010 la comunidad internacional difícilmente hubiera considerado a un portal web como una amenaza para la paz y seguridad internacionales. El fenómeno *WikiLeaks* demuestra que las TIC han transformado el modelo diplomático tradicional. Hoy en día, la secrecía y confidencialidad, características de la diplomacia, se encuentran en proceso de redefinición. La práctica tradicional enfrenta nuevos desafíos debido al creciente uso de nuevas tecnologías; en consecuencia los organismos estatales deberán incorporar a la práctica dichas herramientas informáticas.

Actualmente las personas no sólo son capaces de comunicarse entre sí a través de grandes distancias también pueden interactuar con sus gobernantes, intercambiando opiniones sobre determinados asuntos, demandado soluciones e incluso denunciando actividades ilícitas. *WikiLeaks* surge en este contexto como una organización sin fines de lucro dedicada a denunciar actividades ilegales, casos de corrupción e impunidad por parte de mandatarios, personajes políticos, corporaciones, organizaciones religiosas, entidades financieras, etc. Sus principales objetivos son la transparencia institucional y la libre expresión, su funcionamiento es posible gracias a la colaboración de informantes que desean hacer públicas determinadas irregularidades facilitando pruebas documentales. Si bien las filtraciones siempre han existido en el ámbito internacional, nunca habían ocurrido a esta escala. El impacto provocado se debe, en gran parte, al uso de nuevas tecnologías cuyos alcances aún se desconocen en su totalidad.

Los países deben mejorar la interacción gobierno-sociedad, estableciendo una comunicación abierta y constante con la ciudadanía. En una época en donde la información es esencial la

sociedad no puede mantenerse al margen de lo que acontece en el mundo, hoy día los ciudadanos están al tanto de la actividad política de su país y de la de otros Estados. Como resultado cada día surgen nuevas organizaciones civiles y grupos activistas dedicados a dar proyección a las demandas que las autoridades se niegan a atender, ayudadas en buena medida de la enorme difusión que les brindan las innovaciones tecnológicas. También aparecen agrupaciones en línea, personas que desde distintas partes del mundo se unen y actúan por una causa común. De esta forma cada día aparecen sitios inspirados en *WikiLeaks* con el ideal de mantener un gobierno abierto y honesto, basándose en la transparencia institucional y en el derecho a la información.

Las repercusiones en el terreno diplomático son innegables, pues se ha revelado un campo de acción totalmente diferente. Por tanto es necesario adoptar nuevas formas de comunicación entre representantes diplomáticos y entre éstos con la ciudadanía. El modelo tradicional de comunicación "de arriba hacia abajo" parece obsoleto en una sociedad donde las TIC permiten intercambiar datos en tiempo real y sin límites de alcance y contenido. En la actualidad la sociedad se encuentra internacionalmente más conectada, las decisiones políticas que se toman del otro lado del globo son del conocimiento mundial en cuestión de segundos. Como consecuencia la diplomacia debe incluir nuevas prácticas, no sólo para funcionar de forma eficiente también por su propia seguridad. *WikiLeaks* demostró que hasta los gobiernos más protegidos son susceptibles al robo de información. La práctica diplomática siempre ha representado un elemento esencial para cualquier Estado, por lo que protegerla significa salvaguardar también la seguridad nacional. Los gobiernos buscarán nuevas medidas de regulación cibernética, y reforzarán las orientadas a la protección de comunicaciones diplomáticas, sin embargo Internet seguirá siendo un espacio intangible, descentralizado y de enormes alcances. El ambiente diplomático tradicional ha sido transformado con la llegada de la Era informática.

Entidades similares a *WikiLeaks* continuarán surgiendo en el escenario mundial y es difícil afirmar en qué medida la publicación de filtraciones beneficia o perjudica a la sociedad, no obstante este caso lleva a considerar la participación de nuevas entidades en la política internacional gracias a que Internet les ha otorgado un nuevo espacio para comunicarse. La diplomacia se asemeja a un ser vivo, que se desarrolla y desenvuelve en

nuevos terrenos, que avanza y evoluciona hacia nuevas prácticas, el reto para los Estados es aceptar este cambio, buscando mantener la efectividad y eficiencia de su aparato diplomático.

3.1. Antecedentes

Es importante analizar el papel que las fugas informáticas han desempeñado a lo largo de la historia contemporánea, antes de que Julian Assange ideara un portal dedicado a las filtraciones casos similares ya habían ocurrido a través del tiempo (véase tabla 3).

Tabla 3. Casos de espionaje y filtraciones en la historia

Año	Caso	Actores	Contenido
1971 – 1974	**Los papeles del Pentágono** o Informe McNamara	• Anthony Russo (empleado de Rand Corporation) y Daniel Ellsberg (analista del Pentágono y compañero de Russo) • *The New York Times* • Administración Nixon	Detalles sobre la participación estadounidense en Vietnam. El informe tenía como objetivo explicar la derrota de EE.UU. Consta de 7000 páginas entre cables, telegramas y documentos altamente confidenciales. Incluye datos sensibles como la cantidad de soldados caídos en combate. Sánchez Hernández (2011).
1972 – 1974	**El Watergate** Se denomina así porque es el nombre del hotel en donde iniciaron los hechos.	• Richard Nixon • Egil Krogh, John Erickman, Bob Haldeman, John Mitchell, entre otros. • Bob Woodward y Carl Bernstein • *The Washington Post* • "garganta profunda", informante anónimo, más tarde identificado como William Mark Felt, segundo al mando del FBI. Calvo (2005).	Se trata de un caso de espionaje organizado en la Casa Blanca durante el mandato de Richard Nixon. Woodward y Bernstein se dedicaron a investigar un supuesto caso de robo en la oficina electoral del Partido Demócrata, el resultado fue el mayor escándalo de espionaje en la historia de Estados Unidos y que obligó a Nixon a renunciar a la presidencia en 1974. Alba (1974).
1972 -1982	Las publicaciones **Jack Anderson**	• Jack Anderson • *The Washington Post*	Se trataba de una columna en *The Washington Post* encargada de revelar casos de corrupción. Las fuentes de Anderson siempre permanecieron en el anonimato.

2003 – 2004	Los abusos en **Abu Ghraib**	• Los sargentos Michael Smith y Santos Cardona • El cabo Charles Graner • El soldado Joseph M. Darby • *The Washington Post*	*The Washington Post* publicó una serie de fotografías que evidenciaban los abusos en la prisión de Abu Ghraib (situada a 32 kilómetros de Bagdad). En las imágenes se podía observar a militares estadounidenses torturando prisioneros. El soldado Joseph M. Darby entregó a los mandos militares un CD con las fotografías. Hersh (2004).
2002 – 2008	**El Plamegate**	• Valerie Plame (agente de la CIA) • Joseph C. Wilson (ex embajador) • Altos funcionarios de la administración Bush como: Karl Rove (asesor presidencial), Lewis "Scooter" Libby, Ari Fleischer, entre otros.	En esta ocasión se filtró el nombre de una agente de la CIA a los medios de comunicación, según diversas fuentes altos mandos de la administración Bush estaban involucrados. La acción fue en represalia por las críticas que el esposo de Valerie Plame realizó al régimen de George W. Bush, a través del artículo "Lo que no encontré en África" publicado por *The New York Times* en él manifestó que Bush había manipulado los datos que presentó después de haber viajado a Níger para investigar las intenciones de Iraq para obtener uranio. García y Staudacher (2008).

Fuente: Elaboración propia.

Históricamente las filtraciones han representado una herramienta a favor de la transparencia y la justicia social, se trata de informantes que proporcionan datos de forma anónima (por lo general) para evidenciar casos de corrupción e injusticias; sin embargo, también pueden perseguir intereses particulares; en este sentido la labor periodística resulta esencial. Para los periodistas es muy importante comprobar los datos proporcionados, pues se trata de información muy delicada que será presentada a la ciudadanía. Por parte del espectador, éste debe adoptar una posición crítica y exigir fuentes sólidas que sustenten la publicación. De parte de las instituciones u organismos públicos y privados, la seguridad en sus comunicaciones y bases de datos es un asunto fundamental; cualquier institución en especial gubernamental adoptará las medidas necesarias para evitar fugas de información debido a que manejan asuntos vitales para el bienestar social, y para el de la propia nación. Sin embargo, cuando la rendición de cuentas se convierte en una labor opcional y no obligatoria las fugas informáticas son ampliamente aceptadas por la sociedad, ya que comparten datos que de manera general se ocultan a la ciudadanía y exponen la forma real

en que trabajan los Estados. Empero, no se debe olvidar que la privacidad en las comunicaciones y datos de una nación es una cuestión delicada, pues está directamente relacionada con la seguridad nacional. Cuando información militar, económica y diplomática se encuentra al alcance de todo el mundo se vulnera la seguridad del Estado, por lo que es muy importante establecer una comunicación equilibrada y constante entre ciudadanos y gobernantes.

A través del tiempo han existido diversos casos de fugas informáticas que han logrado generar importantes repercusiones, el caso de Daniel Ellsberg es un ejemplo. Ellsberg era un analista militar, formaba parte del sistema que más adelante se encargaría de desafiar; se enfrentó por un lado a lo que individualmente consideraba correcto, y por el otro, a las acciones que su país llevaba a cabo en Vietnam. En junio de 1971 Ellsberg filtró un informe altamente confidencial a la prensa sobre la guerra estadounidense el sudeste asiático, el informe McNamara estaba conformado por cables, telegramas y documentos clasificados.[78] También conocido como *The Pentagon Papers* (los Papeles del pentágono), fue uno de los primeros y más famosos casos de filtración periodística en la historia que causó reacciones en la sociedad y en todo el mundo, tanto a favor como en contra. La figura de los *whistleblowers* (informantes) siempre ha sido polémica, tanto que en su momento Ellsberg fue considerado traidor. Las filtraciones demuestran la falta de transparencia institucional y una comunicación ineficiente entre los gobernantes y los ciudadanos.

Otro caso simbólico es el Watergate. En esta ocasión la labor periodística fue más ardua, pues no se trataba de un informe final, listo para su publicación; los reporteros de *The Washington Post* contaban sólo con pistas. La mayor parte del trabajo les correspondió a los periodistas Bob Woodward y Carl Berstein,[79] además la identidad del informante, en ese entonces, era desconocida. Esta vez la sociedad comenzó a involucrarse más en el funcionamiento de su gobierno, a tal grado que la creciente presión social provocó que el presidente Richard Nixon renunciara a su cargo a mediados 1974.[80] El escandalo Watergate es

[78] Sánchez Hernández, Carlos. (2011). "Analogías de la Historia I: Julian Assange y WikiLeaks vs Daniel Ellsberg y los PentagonPapers". *Nómadas*, no. 31. [En línea]. Disponible en: <http://www.redalyc.org/src/inicio/ArtPdfRed.jsp?iCve=18120621004>. (Consulta 11/11/2013).
[79] Sánchez Hernández, Carlos. (2005). "Treinta años después del Watergate (1974-2004)". *Nómadas*, no. 11. [En línea]. Disponible en:<http://www.redalyc.org/articulo.oa?id=18101106>. (Consulta 21/02/2013).
[80] *Ídem.*

clave no sólo para el ámbito periodístico nacional sino también para el internacional, ya que demostró lo que la opinión pública es capaz de lograr y reflejó la necesidad de una administración honesta y una interacción más cercana con las autoridades.

En el siglo XXI la evolución de las comunicaciones trajo consigo grandes cambios, la sociedad misma se transformó, cambió la forma de participación ciudadana, incrementó el flujo de información, surgieron nuevos canales de interconexión y nuevas formas de convivencia. Con la llegada de la Sociedad de la información las filtraciones potencializaron sus alcances.

En 2003 se conocieron los abusos en Abu Ghraib. Fue la primera vez que las telecomunicaciones estaban directamente involucradas, pues las imágenes fueron presentadas en los medios clásicos y en la red. Las fotografías revelaban la violación de derechos humanos en una prisión de Bagdad. En un primer momento no hubo informantes, las imágenes fueron introducidas directamente en la red de comunicación global, circuló por distintos ordenadores hasta que el soldado Joseph M. Darby entregó un CD con las imágenes a las autoridades militares.[81] El impacto generado en la sociedad fue evidente: gobiernos, organizaciones no gubernamentales y organismos internacionales se pronunciaron al respecto. Las deficiencias del sistema fueron evidenciadas a escala mundial.

La web constituye un punto de encuentro entre individuos de todo el mundo, aunado a ello la cantidad de información que genera cada día es impresionante. Se trata de una nueva vía de comunicación social capaz de interconectar ciudadanos con sus gobernantes. Dado que el sistema internacional está compuesto por entidades en constante comunicación, y que durante los últimos años las comunicaciones se han transformado, el sistema internacional ya no es el mismo. Hoy por hoy las personas pueden estar virtualmente presentes en distintas partes del mundo, la barrera espacio-tiempo es cada vez más imperceptible, como consecuencia día con día surgen nuevas organizaciones sociales que demandan mayor participación en la dinámica internacional. Cada individuo se ha convertido en una especie de espectador mundial capaz de comunicarse con entidades nacionales e internacionales. La Relaciones Internacionales están entrando en una nueva etapa de interacción, al tiempo en que surgen nuevos participantes.

---

[81] Hersh, Seymour. (Mayo 10, 2004). "Torture at Abu Ghraib". *The New Yorker*. [En línea]. Disponible en: <http:// www.newyorker.com/archive/2004/05/10/040510fa_fact>. (Consulta 10/03/2013).

Con la llegada de la Era informática y el creciente uso de redes sociales aparecieron diversos portales y movimientos a favor de la transparencia o con el fin de evidenciar injusticias e irregularidades en todo el mundo, iniciativas por parte de organizaciones no gubernamentales, la sociedad civil o grupos activistas (véase tabla 4). Los sitios web dedicados a las filtraciones y al activismo político pueden representar una oportunidad para la sociedad o un desafío para los Estados.

Tabla 4. Organizaciones activistas en la red

Portal	Misión / Características
100Reporters.org	Tiene como objetivo incrementar el impacto y la calidad del periodismo de investigación, y de las denuncias ciudadanas en todo el mundo. Está conformada por diversos reporteros e informantes de distintas partes del mundo.
Crocodyl.org	Apoya el trabajo de pequeños grupos activistas que se enfrentan a importantes multinacionales en busca salvaguardar los derechos humanos y el equilibrio ambiental. Su principal objetivo es promover la responsabilidad corporativa. El portal web permite a los usuarios editar y agregar datos—noticias de última hora, denuncias, etc.— conservando la calidad y la autenticidad gracias a la revisión de editores y expertos. Utiliza la sabiduría colectiva de los "vigilantes corporativos" para mantener compañías e industrias con altos índices de rendición de cuentas.
Cryptome.org	Funciona como depósito para la información que es censurada por las autoridades, y que está relacionada con temas como libertad de expresión, criptografía, espionaje, vigilancia, seguridad nacional, agencias de inteligencia, etc. Hasta el día de hoy ha revelado cerca de 74 000 archivos. Cuenta con sub áreas especializadas.
Corruptionwatch.org.za	Se trata de un portal de denuncias para exigir mayor transparencia por parte de líderes políticos. Desea que quienes manejan los recursos públicos sean responsables y actúen a favor del bienestar común, promueve la transparencia y la rendición de cuentas, su objetivo es proveer herramientas a la sociedad civil para combatir la corrupción. Cuenta con herramientas como una línea SMS, redes sociales, correo electrónico y el propio portal para recibir denuncias ciudadanas; posteriormente se dedican a investigar y a reportar a las autoridades los casos recibidos. Busca mejorar la democracia, el estado de derecho, y establecer una sociedad más atenta y justa. El financiamiento proviene de donaciones de organizaciones internacionales, instituciones públicas y privadas, y de particulares.

oecd.org/daf/anti-bribery/	Orientada a combatir el soborno en el comercio internacional, y apoyar el progreso; tiene como objetivo reducir la pobreza y robustecer la confianza en los mercados. Su principal fundamento es la Convención anti cohecho de la OCDE (de 2009) y está conformada por programas especiales en África, Asia-pacifico, Europa oriental y Asia central, y Latinoamérica. El sitio también ofrece publicaciones y estudios sobre el combate a la corrupción y su estado en diversos países, busca fortalecer la aplicación (y cumplimiento) de diversos acuerdos anticorrupción, tanto nacionales como internacionales.
Publicintelligence.net	Es un proyecto internacional de investigación que reúne el trabajo de especialistas independientes que defienden el libre acceso a la información de interés público, pues consideran que constituye un derecho humano; concibe a la transparencia como un factor determinante en la democracia, y rechaza el control de datos por parte de instituciones, regímenes y corporaciones con el fin de manipular la opinión pública. Protege los datos de interés general por medio de software y métodos de código abierto al alcance de todos, busca generar una sociedad informada y activa, publicando documentos, análisis y reportes del sector público y privado. Sus escritos han sido utilizados por medios de comunicación internacionales y por *think thanks* de distintas partes del mundo.
Revenuewatch.org	Es una organización sin fines de lucro dedicada al diseño de políticas sustentables además brinda asistencia y financiamiento a favor de una gestión eficaz, transparente y responsable de recursos petroleros, gasísticos y minerales. Se especializa en países con abundantes recursos naturales que generalmente (debido a sus altos índices de pobreza) se enfrentan a diversos problemas como la corrupción y los conflictos armados, fomenta la capacitación, asistencia técnica y la investigación en el sector energético y minero. Su principal cede se encuentra en Nueva York y tiene representaciones en Londres, Ghana, Azerbaiyán, Nigeria, Indonesia, Tanzania y Perú. En la actualidad trabaja en más de 30 países brindando apoyo financiero y técnico a cerca de 50 organizaciones relacionadas con petróleo, gas y minería, también colabora con instituciones académicas para brindar una mejor orientación entorno a mecanismos de explotación sustentable. Trabaja con entidades internacionales como el Fondo Monetario Internacional y el Banco Mundial.
Transparency.org	Está presente en más de 100 países y cuenta con sede principal en Berlín, se define como un movimiento internacional en busca de un mundo en el que gobierno, empresas y sociedad estén libres de corrupción. Sus valores son la transparencia, la rendición de cuentas, la integridad, la solidaridad, el valor, la justicia y la democracia. Entre sus principales logros están: 1) la creación de convenciones internacionales anticorrupción; 2) la denuncia de líderes corruptos; 3) el monitoreo de elecciones nacionales, y 4) mantener empresas responsables en el plano nacional e internacional. Es políticamente independiente y se sostiene gracias a donaciones.

Worldbank.org (por el derecho a la información, a la transparencia y a un gobierno abierto)	A favor del fácil y libre acceso a la información relacionada con políticas, gastos y al proceso de toma de decisiones gubernamentales. Busca un Estado transparente y responsable. Cuenta con un grupo por la Gobernabilidad del Sector Público, PREM (por sus siglas en inglés), que se encarga de desarrollar estudios y recursos que ayuden a las instituciones públicas a mejorar la transparencia y el libre acceso a la información. Comparte documentos relacionados con transparencia gubernamental como: mecanismos para la rendición de cuentas, investigaciones sobre iniciativas eficaces, tecnologías a favor de la transparencia, datos acerca de leyes sobre libertad de expresión, estadísticas, análisis por regiones, conferencias, etc.

Fuente: Elaboración propia.

Desde finales del siglo pasado han surgido portales web en contra de injusticias y corrupción; a favor de la transparencia institucional, la democracia, etc. Lo más importante es que estas entidades —además de estar conformadas, en su mayoría, por ciudadanos de todo el globo—orientan su trabajo en áreas específicas. Internet permite que la sociedad, gobiernos, organizaciones no gubernamentales y organismos internacionales establezcan conexiones entre sí. Un ejemplo, es el portal de la Organización para la Cooperación y el Desarrollo Económicos (OCDE)[82] encargado de combatir la corrupción e impulsar el progreso; esta clase de instituciones sirve a la ciudadanía como una especie de vigilante internacional. Del mismo modo existen otras entidades dedicadas a la rendición de cuentas por parte de los gobernantes, que se han vuelto transcendentales en la arena internacional.

Un caso más, son los sitios web como *Cryptome.org* que trabajan a favor del libre flujo de información. Dado que el ciberespacio es un lugar intangible y de enormes dimensiones es difícil pensar que conceptos como censura y represión posean los mismos alcances que tenían en el siglo pasado; no obstante la *Word Wide Web* continúa dependiendo de dispositivos físicos para funcionar. Sin embargo, a pesar de que es posible establecer fronteras y restricciones dentro y fuera de la red, el alcance de sus dimensiones es todavía incontrolable. Espacios como *Cryptome* se presentan como plataformas para la difusión de información relevante que habitualmente es censurada por los Estados. De cierta forma son los sucesores de las pequeñas imprentas y editoriales que durante el siglo XX intentaban sobrevivir en contra de regímenes poco transparentes y represivos. La expresión de distintas opiniones se ha digitalizado e

[82] *OCDE*. "Bribery in international business". [En línea].Disponible en: <http://www.oecd.org/daf/antibribery/>. (Consulta 13/07/13)

internacionalizado, pues la web está presente en todo el mundo, sirve como herramienta a los ideales de transparencia y denuncia social, y ayuda a difundir información que algunas autoridades preferirían ocultar.

Otro caso significativo es *Revenuewatch.org* especializada en la gestión eficaz de recursos naturales, que trabaja a favor de la sociedad y del medio ambiente. De la misma forma que *Revenuewatch* está orientada a proteger el entorno, también existen entidades dedicadas a distintas áreas como la protección de pueblos indígenas, el combate del hambre y el cabildeo a favor de los derechos humanos, etc. En la actualidad un ciudadano, testigo de alguna injusticia, puede tomar su ordenador, enviar el mensaje a través del ciberespacio, y en cuestión horas, miles de personas alrededor del mundo se suman a la causa. En la aldea global gracias al trabajo conjunto la intensión puede convertirse en acción. Estas organizaciones también han logrado diversificar sus relaciones, pues hoy día interactúan con otros organismos no gubernamentales e instituciones internacionales; por ejemplo, *Revenuewatch* trabaja con el Fondo Monetario Internacional y el Banco Mundial.

Todos los días la red de redes extiende sus enlaces e interconexiones a lo largo del mundo, gracias a ello las ciberorganizaciones activistas han obtenido mayor proyección y también han logrado nutrirse del conocimiento colectivo. Por su parte el usuario tiene acceso a múltiples informes, estadísticas y datos especializados que difícilmente hubiera podido obtener en épocas anteriores. Si hay algo que es común en estos organismos es que la mayoría se pronuncia a favor de un gobierno honesto y abierto, dirigentes responsables, la libre expresión, la democracia, la protección al medio ambiente y del bienestar común; combaten el soborno, la corrupción, la injusticia y la censura. Aunque todos estos ideales ya existían fue gracias a Internet que dicha voz potencializó sus alcances. Hoy en día cada decisión u omisión por parte las autoridades es examinada por dichas entidades, que al estar en constante contacto con la ciudadanía —elevando el flujo de información en ambos sentidos— incrementan el peso de la opinión pública.

Las TIC han transformado la dinámica mundial, la diplomacia debe tener en cuenta que su entorno ha sido modificado por el surgimiento de nuevos canales de interacción, esta pluralidad trae consigo nuevas ideas y oportunidades. La comunicación oficial está

transitando de un modelo unidireccional a uno con múltiples canales, caracterizado por la incorporación de nuevos actores en la dinámica internacional.

El activismo en Internet aumenta considerablemente día a día, la web representa un nuevo espacio público en el que habitantes de todas partes del mundo coinciden en un mismo espacio y tiempo, y pueden interactuar entre sí o con sus gobernantes. Poco a poco distintas naciones han ido incrementando su presencia en el ciberespacio, mientras que otras optan por restringir el acceso a éste.

3.2. Surgimiento de *WikiLeaks*

WikiLeaks surgió en 2006, aunque su fundador Julian Assange contemplaba su creación desde1999,[83] Assange ideaba una web que ayudará a terminar con las injusticias del mundo, en un blog creado en *IQ.org* declaró:

> *Cuan más secreta es una organización, más miedo y paranoia generan las filtraciones. Debido a que los sistemas injustos llevan por naturaleza a la creación de una oposición, las filtraciones masivas los dejan exquisitamente vulnerables y los amenaza con formas más abiertas de gobernabilidad.*[84]

El 14 de noviembre de 2006 Julian Assange compartió a los lectores de su portal la idea de un nuevo proyecto: *WikiLeaks*.org.[85] Un sitio que serviría como plataforma para dar a conocer filtraciones relacionadas con casos de impunidad y corrupción de regímenes, corporaciones, instituciones internacionales, entidades financieras y organizaciones religiosas alrededor del mundo. Los documentos confidenciales se obtendrían por medio de informantes anónimos que contactarían a la organización a través de sistemas informáticos que protegerían la identidad de la fuente, en seguida los datos serían analizados y comprobados para, por último, colocarlos en dicho portal. *WikiLeaks* tiene como objetivo lograr instituciones transparentes, defender el derecho a la información y mantener un gobierno abierto. Se conforma de voluntarios de todo

[83] Leigh, David y LukeHarding. (2011). *WikiLeaks, Inside Julian Assange's War on Secrecy*. Reino Unido: Guardianbooks.
[84] Boix, Leonardo. (Febrero, 2011). "Cuando los secretos se odian". *Proceso,* no. 1788.
[85] *Ídem.*

tipo: activistas, ingenieros, matemáticos, arquitectos, etc. Financieramente se sostiene gracias a donaciones procedentes de distintas partes del mundo.[86]

Para conservar la confidencialidad de las fuentes *WikiLeaks* utiliza el sistema 256 bit que es un método avanzado de encriptación similar a la que utilizan algunos bancos y militares y de inteligencia, por su parte el portal electrónico funciona a través de una conocida como MediaWiki.[88] *WikiLeaks* estructuralmente está compuesta por un Consejo asesor, una Junta consultiva y un Editor jefe (Julian Assange), al respecto aunque por razones de seguridad no se ha revelado la identidad de todos sus miembros es posible mencionar algunos de ellos: Wang Dan, (miembro del Consejo asesor) activista por la libertad y la democracia en China; Francisco Whitaker Ferreira, (miembro de la Junta consultiva) arquitecto, político y activista social en Brasil, y Ben Laurie, (miembro de la Junta consultiva) ingeniero de software, diseñador de protocolo, criptógrafo y activista.[89]

De acuerdo con Valérie Guichaoua (2011), la postura política de *WikiLeaks* va más allá de "izquierda" o "derecha", su lucha es específicamente en contra del individualismo y de las instituciones corruptas, y su trabajo se orienta al establecimiento de gobiernos éticos y abiertos.

Los recursos económicos de la organización provienen de donaciones vía electrónica (MasterCard, Visa y PayPal). En 2010 Julian Assange declaró que *WikiLeaks* contaba con un presupuesto anual de aproximadamente un millón de dólares. Sin embargo, al momento de su lanzamiento la organización sobrevivió gracias a las aportaciones de Assange y otros miembros.[90]

---

[86] *Ídem.*

[87] También conocido como Rijndael, es un esquema de cifrado por bloques adoptado como estándar de cifrado por el gobierno de Estados Unidos. Desde 2006 el AES es uno de los algoritmos más populares usados en criptografía simétrica.Fuente: Beckett, Charlie y James Ball. (2012). *WikiLeaks: News in the Networked Era*. Reino Unido: Polity Press.

[88] MediaWiki es un software libre escrito originalmente para Wikipedia, ahora es utilizado por otros proyectos de la Fundación Wikimedia y por otros portales. Fuente: Miller-Jones, Edward R. (2010*). WikiLeaks, Removing the 'top secret' seal.* Estados Unidos: Fastbookpublishing.

[89] Miller-Jones, Edward R. *Óp. Cit.*

[90] Bravo A., Mauricio. (2013). *WikiLeaks: teoría y práctica de un desacato*. Santiago de Chile: Ediciones Nueva Fojas Ltda. [En línea]. Disponible en: <http://alainet.org/images/Wikibook.pdf>. (Consulta 11/05/2014).

En diciembre de 2010 Mastercard y Visa bloquearon las cuentas bancarias de *WikiLeaks*, y tras meses de litigio finalmente se restableció el servicio.[91] A pesar de diversas complicaciones económicas *WikiLeaks* ha logrado mantenerse a flote gracias al apoyo de diversos grupos activistas, en especial gracias el trabajo de la fundación *Wau Holland Stiftung*[92] quien se encarga de recibir donaciones a *WikiLeaks* provenientes de Europa.[93] De acuerdo con el reporte más reciente (de julio de 2012) *WikiLeaks* recibió aproximadamente 200 000 euros mensuales por concepto de donaciones.[94]

El portal fue presentado de manera oficial en enero de 2007, durante el Foro Social Mundial Mundial celebrado en Nairobi, Kenia. En aquel entonces publicó una serie de reportes que revelaban un fraude de cerca de mil 500 millones de euros por parte del ex Presidente keniano Daniel ArapMoi. La filtración se produjo a sólo unos días de celebrar elecciones, y sin duda jugó un papel fundamental para que Raila Odinga, líder demócrata, ocupara el cargo de primer ministro, una vez que el candidato Kibaki (apoyado por ArapMoi) fuera elegido presidente.[95]

En adelante se dedicó a evidenciar problemas de corrupción en distintos Estados, irregularidades en prisiones e incluso el asesinato de corresponsales de guerra. Sus últimas revelaciones consisten en bitácoras de operaciones militares en Afganistán y comunicaciones diplomáticas entre funcionarios de distintas partes del mundo, ambas pertenecientes al gobierno estadounidense. Además en 2012 publicó más de dos millones de correos electrónicos relacionados con el régimen sirio.

3.3. Ética hacker, periodismo y *WikiLeaks*

Antes de continuar con este apartado es preciso definir qué es el *hacking* y quiénes lo desarrollan. Es importante señalar que, aunque posee una amplia variedad de significados,

---

[91] AP. (Julio 13, 2012). "WikiLeaks gana round a Visa y MasterCard". *El Economista*. [En línea]. Disponible en: <http://eleconomista.com.mx/tecnociencia/2012/07/13/wikileaks-gana-round-visa-mastercard>. (Consulta 11/05/2014).

[92] Creada en 2003 en memoria del científico computacional del mismo nombre, su sede principal se encuentra en Alemania.

[93] Muñoz, Alonso. (2010). "Wikileaks, mucho más que Julian Assange". *Diagonal*. [En línea]. Disponible: <http://www.diagonalperiodico.net/Wikileaks-mucho-ma-s-que-Julian.html>. (Consulta 11/05/2014).

[94] Wau Holland Stiftung. (2012). *WikiLeaks/Project 04: Monthly Balance 2010-2012*.Wauland. [En línea]. Disponible: <http://www.wauland.de/files/2010-2012_Projekt04-Balance.pdf>. (Consulta 11/05/2014).

[95] "WikiLeaks, todo lo que necesitas saber" (Septiembre 21, 2010) *genbeta*. [En línea] Disponible en: <http://www.genbeta.com/activismo-online/wikileaks-todo-lo-que-necesitas-saber>. (Consulta 26/02/2013).

generalmente se relaciona con la irrupción ilegal a un programa informático o sistema de trabajo. Para Santiago Acurio Del Pino (2008), el *hacking* consiste en acceder (desde algún lugar del ciberespacio) a un ordenador privado valiéndose de deficiencias en los sistemas de seguridad, aprovechando su vulnerabilidad, u obteniendo contraseñas de acceso haciéndose pasar por usuarios legítimos. Según Peter G. Neuman (1984), científico en computación, el *hacking* es una intromisión maliciosa que trata de hurgar entre datos buscando información valiosa. Por otro lado, Eric S. Raymond, experto en el ámbito, define al *hacker* como "[…] persona que disfruta aprendiendo detalles de los sistemas informáticos y desarrollando sus capacidades […]".[96]

De acuerdo con Steve Levy, autor de *Hackers: Heroes of computer revolution*, los primeros *hackers* fueron estudiantes del Instituto Tecnológico de Massachusetts, MIT (por sus siglas en inglés). Según Levy el *hacking* va más allá de las actividades ilegales con las que se asocia el término hoy en día, en un principio fue una actividad de élite, ejecutada por individuos altamente calificados cuyo principal motivo era el deseo de aprender, más que el simple propósito de hacer daño. Erik Brunvand, de la universidad de Utah, define este periodo como "la época de oro del *hacking*" (entre los años 1950 y 1960)[97] que tuvo lugar principalmente en el MIT y la Universidad de Stanford, en California.[98]

Los motivos para realizar *hacking* son diversos, mientras unos declaran que es mera curiosidad; otros, que el propósito es mostrar las debilidades de un sistema. Esta práctica, como muchas otras, se rige por una especie de normatividad, identificada como *ética hacker* respecto a la que existen opiniones encontradas. Por un lado se afirma que el *hacking* es ético, siempre y cuando no produzca daños significativos, y por otro lado, están quienes sostienen que cualquier irrupción ilegal a un sistema es perjudicial, y por lo tanto carente de ética. Algunos miembros de la comunidad *hacker* afirman que la ética se determina por las acciones y no por los resultados, de esta forma el fin no justifica los medios; por lo tanto, aunque se lleve a cabo para defender causas justas, el *hacking* de ninguna forma puede ser moral. Del otro lado, están quienes afirman que realmente existe una ética que guía sus

[96] Kenneth Einar, Himma. (2007). *Internet Security, hacking, counterhacking, and society*. Estados Unidos: Jones and Bartlett Publishers, p. 7.
[97] Brunvand, Erik. (1996). "A Little Bit of Hacker History". *Hacker Folklore Page*. [En línea] Disponible en: <http://www.cs.utah.edu/~elb/folklore/afs-paper/node3.html>. (Consulta 29/03/2013).
[98] Kenneth Einar. *Óp. Cit.*

acciones y justifica la irrupción a sistemas privados; desde este punto de vista toda información debe ser libre, los defensores de esta proposición se oponen a cualquier tipo de restricción, protegiendo el libre acceso a la información; Richard Stallman, programador estadounidense, en su manifiesto GNU (movimiento a favor de conocimiento y software libres) apoya la idea de que la información debe ser para todos y ha señalado que, puesto que la información es libre, no deberían existir conceptos como la propiedad intelectual y los derechos reservados.[99]

En 1984 Steve Levy enumeró los principios fundamentales de la ética *hacker*: 1) el acceso a los ordenadores debe ser total e ilimitado; 2) toda información debe ser libre; 3) es preciso desconfiar de la autoridad, debe promoverse la descentralización de la información; 4) los *hackers* deben ser juzgados por sus acciones y no por falsos criterios como su estatus, edad, origen o posición.[100]

Algunos de los motivos por los que se realiza *hacking,* según Kenneth Himma (2007), profesor de Filosofía en la Universidad de Seattle, son:

- Por cuestiones de seguridad: para demostrar la vulnerabilidad de un sistema o sus debilidades;
- Por inactividad del sistema: porque no se explota totalmente su capacidad;
- Con fines de aprendizaje: entrar a un sistema con el fin de instruirse;
- En pro de la sociedad: irrumpen para descubrir casos de abusos o delitos en contra de la sociedad, manteniendo una especie de vigilancia, en este caso el *hacker* es considerado un protector; esta tendencia es más fuerte en Europa que en Estados Unidos, sin embargo, no es muy claro qué tan efectiva es para solucionar dichas infracciones.

Es necesario analizar si, bajo ciertas circunstancias, el *hacking* es ético o hasta legítimo, como en el caso del *counterhacking* que consiste en llevar a cabo dicha actividad en defensa de un ataque de la misma naturaleza, bajo esta situación se considera un acto de legítima defensa. Kenneth Himma sostiene que es posible, si se toma como base la teoría del Derecho Natural de Thomas de Aquino, de manera que puede ser legítimo generar de manera consciente un daño, si con ello se evita otro mayor.

---

[99] *Ídem.*
[100] *Ídem.*

Específicamente en el *counterhacking*, plantea Himma, existen cinco principios sustanciales referentes a la ética

1. Como medida de defensa- En defensa propia, o en la de otros. Se puede utilizar la fuerza (entiéndase aquí como actividad *hacker*) de manera legítima cuando es necesaria para defenderse de un ataque, ésta debe ser proporcional a la que es utilizada en su contra y sólo la necesaria para repeler el o prevenir el ataque, así mismo se dirigirá sólo a quienes estén directamente involucrados.
2. Cuando es preciso hacerlo- Con el fin de alcanzar un beneficio moral mayor. Puede permitirse que una persona (A) infrinja los derechos de otra persona (B) si, y sólo si: el resultado es lograr un beneficio moral mayor, si las ventajas de proteger los derechos de B son menores, moralmente hablando, que los que se pueden obtener si se quebrantan, y si no existe otra forma en la que A puede conseguir su objetivo.
3. Como desagravio-También conocido como *evens the score,* permite que una persona pueda causar daño proporcional al que ha recibido. Está permitido que A, inflija daño a B, en la medida en que este último le ha perjudicado
4. Como forma de sanción- Segundo principio bajo la premisa *evens the score*. Es aceptable que una sociedad sancione a un individuo que ha causado agravio. En este sentido la defensa activa es legítima cuando se trata de castigar un ataque.

Himma sostiene que la mayoría de los medios de comunicación tienden a exagerar la actividad *hacker*, y al mismo tiempo la condenan. Sin embargo, la irrupción a sistemas informáticos puede brindar herramientas para mejorar las medidas de seguridad, en adición, en una sociedad democrática el aumento de la población con altos conocimientos informáticos fortalece a la ciudanía; Himma toma como ejemplo el desastre nuclear en Chernóbil, después del desastre algunos miembros del *Chaos Computer Club* del este de Alemania, consiguieron información de interés público sobre proyectos del gobierno alemán en la zona. Otro punto importante es el uso del *hacking* como método de defensa contra el terrorismo, dado que estas actividades cada día recurren más al uso de nuevas tecnologías, el *hacking* podría ser de utilidad para frustrar posibles ataques. Himma declara que un ejemplo es Estados Unidos, donde se ha ofrecido a algunos infractores (*hackers*) formar parte de

organismos de seguridad e inteligencia, proponiéndoles reducir o eliminar sus condenas, y con ello se utilizan las habilidades de estos expertos informáticos en beneficio de la nación.

Cada tecnología puede ser utilizada por diferentes elementos de la sociedad, ya sea con fines de emancipación o de dominación, en este sentido las tecnologías de la información, como propone Kenneth Himma no son una excepción, pues al tiempo que ofrecen una promesa utópica de independencia y libertad, de apertura laboral, de democracia digital, del surgimiento de una comunidad global y de la llamada revolución informática; por otro lado, también representan herramientas de dominio y control, e incluso limitan la libertad de pensamiento. Internet representa un sitio con amplio potencial, en el sentido en que permite una comunicación global sin que, hasta el momento, exista una regulación, al respecto hay quienes afirman que las elites dominantes harán todo lo posible para controlar la *ciberesfera pública.*[101] En los principios expuestos por Levy (véase página 84), los *hackers* otorgan una importancia central a la libertad de información, de esta manera, la concientización política —propia del activismo— y la experiencia técnica en informática —del *hacking*—han dado lugar a lo que hoy día se conoce como *hacktivismo.*

Por otra parte si se toma en cuenta que una de las funciones del *hacking* es servir a la sociedad como medio para obtener y compartir información, promoviendo la transparencia y la libre expresión, es posible entender cómo se relaciona con la práctica periodística contemporánea, específicamente con el periodismo de investigación (PI).

En la actualidad el *hacking* puede proveer importantes recursos informáticos a la actividad periodística, en el caso del PI puede representar una fuente de filtraciones, sin embargo, el corresponsal siempre estará obligado a comprobar la veracidad de los datos proporcionados, de manera que las filtraciones sólo ofrecen una pista para el desarrollo de una investigación más profunda. Un ejemplo de esto, es la revista *The New Yorker* que en mayo de 2013 lanzó una plataforma electrónica para recibir denuncias anónimas.

[101] Kenneth Einar, Himma. (2007).*Internet Security, hacking, counterhacking, and society*. EstadosUnidos: Jones and Bartlett Publishers

El sistema fue desarrollado por Aaron Swartz, ex hacker y ciberactivista. Gracias a la colaboración de Swartz, *StrongBox* facilita al periodismo moderno una herramienta capaz de proteger la comunicación entre medios e informantes.[102]

Por lo anterior es preciso analizar brevemente el significado de las filtraciones en el periodismo de investigación. Aunque para algunos profesionales el PI no representa una especialidad, dado que periodismo e investigación son dos conceptos íntimamente relacionados e inseparables, no obstante hay quienes lo definen como:

> *Un tipo de información que es más detallado, más analítico, y que exige más tiempo que la mayoría de la cobertura periodística cotidiana* [...] *tiene por objetivo alcanzar la información oculta, y su temario puede variar ampliamente con el ámbito de la actividad humana.*[103]

Si bien la investigación es parte fundamental del ejercicio periodístico, el PI se distingue por indagar a profundidad, asimismo se encarga de examinar de forma minuciosa sucesos específicos, generalmente relacionados con el interés público. De este modo funciona como denuncia pública, y a la vez constituye una práctica profesional, representa también la importancia de los medios libres como contrapeso a favor de la sociedad.

Un elemento substancial para este tipo de periodismo es la filtración que, de acuerdo con Caminos Marcet (1997), se define como aquella información (de carácter privado) que es facilitada por determinado individuo sobre un asunto de interés público con el propósito de compartirla con todo el mundo. Una vez que es recibida, el periodista debe comprobar la autenticidad e iniciar una investigación más profunda por su cuenta.

Las filtraciones son de gran importancia para el periodismo, puesto que indican el camino a seguir para continuar la investigación, aunque en ocasiones constituyen un aporte significativo no siempre es así, pues los datos obtenidos por este medio pueden no ser auténticos.

---

[102] "New Yorker unveils open source whistleblower system designed by activist Aaron Schwartz". (Mayo 15, 2013), *The Raw History*. [En línea] Disponible en: <http://www.rawstory.com/rs/2013/05/15/new-yorker-unveils-open-source-whistleblower-system-designed-by-activist-aaron-schwartz/>. (Consulta 20/06/2013).

[103] Caminos Marcet, José María et. al. (1997) *Periodismo de investigación. Teoría y práctica*. España: Síntesis.

Con la llegada de las TIC el periodista cuenta con un sinnúmero de recursos informáticos, el objetivo del PI es ir más allá de lo que se puede encontrar en las fuentes comunes. El papel del reportero como contrapeso de los centros de poder tradicional, se ve reforzado por los ideales de transparencia y libre expresión de la corriente *hacker*.

En este sentido, según una declaración en línea, *WikiLeaks* combina las nuevas tecnologías, especialmente las de seguridad, con la práctica periodística y, al igual que el resto de los medios que también ejercen periodismo de investigación, acepta información procedente de fuentes desconocidas. Su relación con la ética *hacker* y el periodismo se refleja en sus ideales de transparencia, justicia y honestidad tanto en los Estados como en otras entidades. La organización afirma que existen regímenes totalitarios en muchas partes del mundo, y que el control y la represión se da hasta en los Estados más democráticos, por lo que, la sociedad cada día requiere con mayor urgencia gobiernos abiertos e instituciones transparentes. De acuerdo con *WikiLeaks*, las filtraciones han logrado cambiar el curso de la historia, produciendo cambios significativos a favor de la sociedad; a través del tiempo, se han utilizado para que gobiernos, empresas e instituciones rindan cuentas de sus acciones, y reconoce que sólo la sociedad podrá obligar a que dichas entidades actúen de forma ética y transparente. Gracias a la adopción y desarrollo de nuevas tecnologías ofrece un método seguro y eficaz para que funcionarios, burócratas y empleados de importantes empresas, compartan información de interés público, sin riesgo a ser descubiertos. *WikiLeaks* señala que los medios, a través de las filtraciones, son capaces de derrotar a los regímenes que se sostienen en mentiras, logrando establecer gobiernos más transparentes. Plantea que gracias a los nuevos métodos criptográficos, los riesgos en el intercambio de mensajes entre periódicos y fuentes han disminuido. La organización se apoya en la resolución de la Suprema Corte de Estados Unidos en el caso de los *Pentagon Papers* en la que se establece: "sólo una prensa libre y sin restricciones, podrá exponer de forma efectiva los engaños del gobierno".[104]

[104] "Should the press really be free?" *WikiLeaks*. [En línea]. Disponible en: <http://wikileaks.org/About.html>. (Consulta 29/06/2013).

Para *WikiLeaks* los regímenes autoritarios, las instituciones opresivas y las corporaciones corruptas no deberían estar sólo bajo la presión de las leyes, la diplomacia o las tendencias electorales, sino de un elemento más poderoso: la opinión pública.[105]

Para finalizar este apartado es posible señalar que la aparición de *WikiLeaks* refleja el alcance de los ideales de justicia, transparencia y honestidad apoyados en las nuevas tecnologías. Al mismo tiempo demuestra que han surgido nuevos actores en el escenario internacional cuyo potencial no se debe subestimar como las organizaciones activistas y los organismos ciudadanos involucrados cada vez más en la interacción entre las naciones, cuya influencia ha crecido considerablemente durante las últimas décadas de auge delas tecnologías de información y comunicación. Vale la pena analizar qué representa el aumento en entidades de esta naturaleza. Si las comunicaciones se han transformado y con ello también la forma en que interactúa la sociedad, los Estados deberán considerar la creación de nuevos espacios de conexión con sus ciudadanos, y adecuar y reforzar los vínculos de interacción entre las naciones.

3.4. ¿Filtraciones o ciberespionaje?

Existe una frecuente discusión en torno a si las actividades de *WikiLeaks* se relacionan meramente con filtraciones periodísticas o si encierran también prácticas de espionaje. Al respecto, es posible decir que dichas actividades poseen significados muy distintos, aunque puede ser que una filtración sea producto de espionaje. Cabe aclarar que *WikiLeaks* se define sólo como una plataforma para difundir filtraciones, y pese a que Julian Assange en su juventud fue un conocido *hacker*[106], no significa que la organización se dedique a intervenir comunicaciones para obtener material. La confusión se debe, en buena medida, a que las autoridades estadounidenses pretendían procesar a Julian Assange bajo la Ley de espionaje de 1917.[107] Por lo anterior es importante analizar en qué consiste una y otra actividad.

---

[105] *Ídem.*

[106] Leigh, David y Luke Harding. (2011). *WikiLeaks: Inside Julian Assange's War on Secrecy*. Estados Unidos: GuardianBooks.

[107] "Julian Assange podría ser procesado de acuerdo a la Ley de Espionaje". (Noviembre 30, 2010) *El Mundo*. [En línea]. Disponible en: <http://www.elmundo.es/america/2010/11/30/estados_unidos/1291142768.html>. (Consulta 23/04/2013).

Respecto a las filtraciones, es posible afirmar que son un elemento característico del periodismo de investigación, y forman parte de la fase de recolección de datos. En este sentido, sentido, independientemente del origen y naturaleza de la información todo periodista está obligado a comprobar su validez, de manera que los datos que se han obtenido por medio de un un infórmate también deben verificarse. Caminos Marcet (1997) señala que en el caso del PI, la PI, la fuente busca al periodista, mientras que en el periodismo convencional, son estos últimos últimos quienes buscan la fuente. De acuerdo con Marcet, una filtración consiste en proveer datos relevates a una investigación, la fuente puede ser anonima o conocida para el periodista —aunque por lo general es desconocida para el público— y puede perseguir diversos intereses. Mientras que para Héctor Borrat, catedrático de la Universidad de Barcelona, consiste en publicar información que se ha obtenido por medio de fuentes cuya identidad se mantiene protegida.[108]

En el ambito periodistico existe un debate respecto a qué tan ético y confiable es acudir esta clase de fuentes, empero no se debe olvidar que gracias a la colaboración de informantes se han revelado importantes casos de corrupción e injusticias a largo de la historia, y que las filtraciones han jugado un papel relevante en la politica internacional.

En algunas ocasiones las filtraciones consisten en datos clave que sirven de guías para orientar el trabajo del periodista, quien realiza la mayor parte del trabajo. Si adoptamos el punto de vista de Marcet es posible diferenciar dos tipos de periodismo, el primero requiere del trabajo del investigador, por ejemplo en el caso Watergate "garganta profunda" proporcionó pistas que Woodward y Berstein debieron descifrar por lo que la investigación les tomó cerca de dos años.[109] En el segundo caso sólo se publica un informe o trabajo terminado, es preciso recordar que en el caso de Daniel Ellsberg *The New York Times* se limitó a publicar, en nueve entregas, un informe final elaborado por el Pentágono.[110]Desde esta perspectiva existe una diferencia importante entre lo que Marcet diferencia como periodismo de investigación y periodismo de filtración; distinguir entre uno y otro es difícil, dado que el carácter confidencial

[108] *Periodismo de investigación: teoría y práctica*. (1997). Síntesis: Madrid. Citado por Caminos Marcet.
[109] Durón García, Carlos. (2013). Columna "Recopilaciones". *La Prensa*. [En línea]. Disponible en: <http://www.oem.com.mx/laprensa/notas/n2904963.htm>. (Consulta 24/06/2013).
[110] Sánchez Hernández. *Óp. Cit.*

de la fuente imposibilita establecer una división entre la información que se obtuvo por cuenta propia, y la que fue proporcionada por informantes.

En la esfera periodística hay quienes adoptan este tipo de fuentes mientras que otros las rechazan por cuestiones morales. Al respecto Caminos Marcet declara: "[…] no existen problemas éticos o deontológicos para la publicación de filtraciones siempre que el haya comprobado la veracidad de los datos filtrados".[111] A pesar de todo, la responsabilidad social del periodista permanece inamovible: informar con apego a la verdad.

Es posible apreciar que la publicación de filtraciones es una cuestión compleja que pone en riesgo no sólo al periodista sino a todo el equipo de trabajo; por esta razón, algunos profesionistas como Lawrence Beaupre director del diario *The Cincinnati Enquire* exigen ciertas condiciones para su publicación como: 1) toda información procedente de fuentes anónimas debe ser comprobada; 2) deben analizarse los motivos que impulsan dicha filtración, para no formar parte de conflictos personales; 3) no utilizar fuentes que realicen juicios de valor sobre otras personas, o expresen opiniones particulares; 4) los datos deben poseer valor periodístico; 5) al igual que en las fuentes *on the record* —información de una fuente cuya identidad se puede publicar—, deberá elegirse la fuente más confiable; 6) debe explicarse al público la razón por la que una fuente permanecerá en el anonimato, y 7) el uso de fuentes anónimas deberá ser aprobado por los responsables de la publicación.[112]

De acuerdo con Marcet (2007) las autoridades son las encargadas de clasificar un documento como "confidencial"; sin embargo, esto no lo exime de ser revelado por los medios de comunicación —los cuales, una vez que los tienen en su poder, decidirán con base en criterios profesionales si deben o no publicarse— ya que en ocasiones los archivos clasificados se relacionan con casos de impunidad e injusticia, y en otros casos se trata de información delicada que involucra cuestiones de seguridad personal y hasta nacional. Respecto a los motivos que generan una fuga de información, Howard Simons, ex director

[111] Caminos Marcet. *Óp. Cit.,* p. 193.
[112] *Ídem,* pp. 187-188.

de *The Washington Post*, señala que las filtraciones se realizan a favor o en contra de un partido político o algún funcionario, o también pueden ser en beneficio de la ciudadanía.[113]

Con base a lo anterior, es posible ubicar a *WikiLeaks* bajo la categoría de periodismo de filtración, pues se encarga de publicar informes y datos proporcionados por fuentes anónimas, anónimas, aunque evidentemente realiza un proceso de investigación y confirmación de datos a datos a diferencia del PI no es él quien dirige el proceso, sino son los datos quienes dirigen la investigación.[114]

Pasando al tema del espionaje, es preciso señalar que representa una actividad antigua incluso más antigua de lo que comúnmente se puede suponer, ante este escenario es difícil establecer la fecha exacta de su aparición, pues el robo o sustracción de información confidencial fue, y continúa siendo, una práctica estratégica en el campo político y militar; por otro lado, existen múltiples interpretaciones acerca de las actividades que engloba, por ejemplo, en el plano nacional el Código Penal Federal lo define como:

- las actividades que cualquier extranjero en tiempos de paz, o de guerra, con el fin de ayudar a una posible invasión tenga relación o inteligencia con otro individuo o cualquier entidad, a la que facilite información, instrucciones o documentos que perjudiquen a la nación;
- al connacional que proporcione datos de un Estado a otro con el fin de ocasionar daño;
- a quien sabe de actividades relacionadas con espionaje y no lo revele a las autoridades.[115]

Según la Organización de Naciones Unidas, el espionaje consiste en:

> […] *la adquisición, la revelación, la transferencia o la utilización de un secreto*
> […] *sin autorización o justificación legítima, con la intención de causar una*

[113] *Ídem.*
[114] *Ídem.*
[115] *Ley de Seguridad Nacional.* [En línea]. Disponible en: <http://www.ordenjuridico.gob.mx/Federal/Combo/C-8.pdf>. (Consulta 24/05/2013).

pérdida [...] *a la persona que tiene derecho al secreto o de obtener un beneficio ilícito para sí mismo o para una tercera persona.*[116]

Con la evolución de las tecnologías de información y comunicación esta práctica también ha transformado, dando lugar a lo que hoy en día se conoce como ciberespionaje que, de acuerdo con Santiago Acurio del Pino (2008), consiste en la fuga de datos o la publicación ilegal de documentos clasificados. Para Acurio del Pino, el constante avance tecnológico convierte al ciberespionaje en una actividad de fácil ejecución que generalmente se combate con mecanismos criptográficos (cifrado de datos)—aunque *WikiLeaks* pudiera entrar en esta clasificación es importante aclarar que el espía es quien sustrae forma directa la información.

Otro aspecto que diferencia al portal de filtraciones son los métodos para obtener datos, ya que mientras *WikiLeaks* funciona como plataforma para recibir aportaciones a través de sistemas de comunicación encriptados, el ciberespionaje utiliza distintos mecanismos para obtener de manera directa los datos, entre ellos: 1) puertas falsas, que consisten en irrupciones a programas informáticos; 2) llave maestra, el uso de un software capaz de introducirse a cualquier archivo, y 3) pinchado de líneas, intervenir las líneas telefónicas en las que circulan datos.[117] En el caso de la organización de Assange no existe ningún vínculo con la entidad o individuo del que se sustrae la información; mientras que en el segundo caso el espía extrae directamente los datos.

Si bien los documentos proporcionados pueden ser producto de espionaje *WikiLeaks* no es la única entidad que ha publicado esta clase de recursos, es posible mencionar diversos casos en los que políticos de partidos contrarios filtran información —obtenida por medio de espionaje— a la prensa con el fin de dañar públicamente la imagen de un funcionario, partido u organización. En este caso la atención se fija en el contenido de la publicación, más que en los métodos con los que se obtuvieron los datos.

---

[116] ONU. (2000). *Décimo Congreso de las Naciones Unidas sobre Prevención del Delito y Tratamiento del Delincuente Viena, 10 a 17 de abril de 2000,* Naciones Unidas, Nueva York, p. 6. [En línea]. Disponible en: <http://www.uncjin.org/Documents/congr10/15s.pdf>. (Consulta 2/06/2013).

[117] Acurio del Pino. *Óp. Cit.*

3.5. Reacción Internacional

En este apartado se analizarán las reacciones generadas en la esfera mundial por lo publicado en *WikiLeaks*. Para ello es importante conocer primero qué opinaban los principales actores respecto a las nuevas tecnologías y su impacto en la sociedad; cómo reaccionaron durante las publicaciones, y por último cuál es su posición ante dichas filtraciones.

En 2003 se llevó a cabo la Cumbre Mundial sobre la Sociedad de la Información en Ginebra, Suiza, por parte de la Organización de Naciones Unidas (ONU) y la Unión Internacional de Telecomunicaciones (UIT) con el propósito de integrar a todas las naciones a la innovación y el desarrollo científico-tecnológico y utilizar dichos avances como instrumento para alcanzar los objetivos del milenio. En la Declaración de Principios de dicha reunión, tanto la ONU como la UIT reconocen que las nuevas tecnologías son necesarias para el progreso y bienestar de la sociedad, y lo más importante, que promueven el diálogo entre personas, naciones y civilizaciones. También plantea que las TIC demandan nuevas formas de solidaridad, asociación y cooperación entre los diferentes actores del escenario internacional. En cuanto a la prensa, señala que los medios libres son un elemento esencial para toda sociedad y declara: "abogamos por que los medios de comunicación utilicen y traten la información de manera responsable, de acuerdo con los principios éticos y profesionales más rigurosos".[118] También hacen referencia a los derechos humanos y las libertades fundamentales, como el respeto al derecho a la privacidad y a la libre expresión de conformidad con los acuerdos internacionales en cada materia.

La Unión Europea (UE) por su parte, establece que las TIC son relevantes para alcanzar los objetivos establecidos en el Tratado de Lisboa —crecimiento elevado, incrementar la tasa de empleo, y la inclusión social—para lo cual creó la iniciativa *e*Europe en 2002. Poco después en un informe titulado "Retos para la sociedad de la información europea con posterioridad a 2005" declara que las innovaciones tecnológicas impulsan la participación ciudadana, y contribuyen a una mayor transparencia y apertura capaz de mejorar la relación entre poderes

[118] ONU, UIT. (2004). *Declaración de Principios, Construir la Sociedad de la Información: un desafío global para el nuevo milenio*. Cumbre Mundial sobre la Sociedad de la Información Ginebra 2003 – Túnez 2005, p. 8. [En línea] Disponible en: <http://www.itu.int/wsis/docs/geneva/official/dop-es.html>. (Consulta 02/06/2013).

públicos y ciudadanos, también señala que debe regularse el desarrollo de dichas aplicaciones para proteger los derechos y la privacidad de toda la comunidad. La UE establece:

> *La difusión cada vez mayor de las TIC fomenta cambios que no se limitan al ámbito de la tecnología. El uso de las TIC crea nuevas modalidades de comunicación e interacción entre los ciudadanos, las empresas y los poderes públicos que abren camino a estructuras sociales y económicas novedosas e instauran nuevas formas de gobernanza.*[119]

En América Latina las TIC representan un instrumento de desarrollo e inclusión social, según la III Conferencia ministerial sobre la sociedad de la información en América Latina y el Caribe, celebrada en Perú (2010). En dicha reunión se estableció un plan de acción a favor del acceso, el desarrollo y la regulación de las nuevas tecnologías en la región. El equipo de trabajo compuesto por Comisión Económica para América Latina y el Caribe (CEPAL) y Observatorio para la Sociedad de la Información en Latinoamérica y el Caribe (OSILAC), comprende que el incremento en el flujo de información no debe limitarse a los miembros de la sociedad, también debe incluir a las autoridades, por lo tanto uno de sus objetivos es establecer un gobierno electrónico, aumentando la cantidad de información disponible para los ciudadanos en la web, y facilitando herramientas y plataformas tecnológicas para obtener una mayor participación ciudadana.[120]

Por parte de Estados Unidos en enero de 2010 la Secretaria de Estado, Hillary Clinton, ofreció un discurso como parte de la inauguración de un museo de periodismo en Washington. En él se refiere a las redes de información como un elemento esencial para la sociedad moderna, y respecto al libre flujo de información en todo el mundo dijo: "las redes de información ayudan a la gente a descubrir nuevos hechos y pedir más cuentas a los

---

[119] UE. (2004). *Retos para la sociedad de la información europea con posterioridad a 2005*. Comisión de las Comunidades Europeas, p. 7. [En línea]. Disponible en: <http://europa.eu/legislation_summaries/information_society/strategies/l24262_es.htm>. (Consulta 03/06/2013).

[120] CEPAL. (2013). *Lista de indicadores para el eLAC2015*. Naciones Unidas, pp. 17-18. [En línea]. Disponible en: <http://www.eclac.cl/publicaciones/xml/2/49212/ListadeindicadoresparaeleLAC2015.pdf>. (Consulta 02/07/2013).

gobiernos". Tanto la Secretaria de Estado como el Presidente Barack Obama abogaban por la libertad de información y expresión en la red en beneficio de los ciudadanos.[121]

Con base en lo anterior es posible observar que la comunidad internacional reconocía la importancia de las nuevas herramientas de comunicación e información, identificándolas como un instrumento útil a favor de la democracia y la libre expresión. Sin embargo, el ciberespacio como todo sitio de convivencia social debe ser regulado, pues no sólo representa un instrumento de comunicación internacional; también, un desafío para todos los Estados especialmente para la actividad diplomática contemporánea.

En noviembre de 2010 *WikiLeaks* publicó 251 287 cables diplomáticos del gobierno estadounidense[122] y las repercusiones le dieron la vuelta al mundo. Se trataban de comunicaciones confidenciales entre representantes de todo el globo, la diplomacia de EE.UU. quedó descubierta a nivel internacional. Como consecuencia surgieron diferentes posturas, desde los que cambiaron radicalmente sus relaciones con Washington (al expulsar a sus diplomáticos), hasta los que señalaron que no informaban nada nuevo. Empero, nunca antes en la historia se habían develado tantos documentos clasificados de una nación; sin duda alguna la práctica diplomática se enfrenta a un importante desafío.

Para entender las diversas reacciones alrededor del caso *WikiLeaks* se han seleccionado algunos casos significativos, dada la exorbitante cantidad de cables publicados, específicamente aquellos que centraron la atención de los medios de comunicación debido a las reacciones y a las medidas tomadas como consecuencia de las filtraciones.

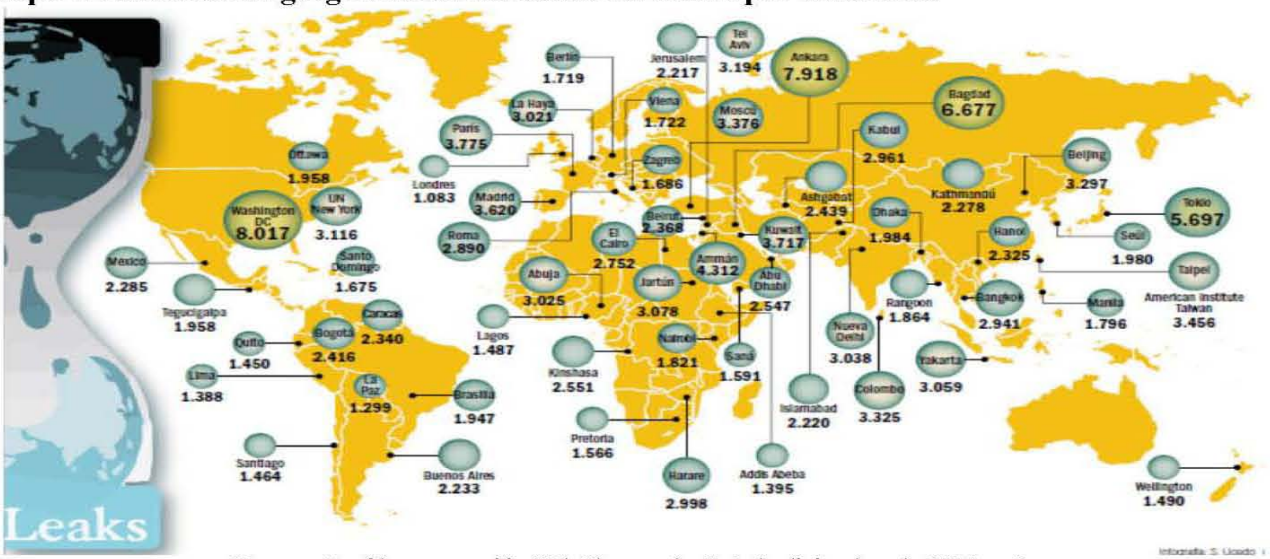
En este sentido, un estudio especializado realizado por el diario electrónico argentino *Perfil.com* muestra qué países fueron los más afectados por las revelaciones dada la concentración de la actividad diplomática estadounidense en determinadas regiones (véase mapa 4).

---

[121] Rodham Clinton, Hillary. (Enero 21, 2010). *Discurso sobre libertad en Internet,* Museo de la Información Newseum, Washington, DC. [En línea]. Disponible: <http://www.state.gov/documents/organization/135880.pd>. (Consulta 16/05/2013).

[122] Leigh y Luke. *Óp. Cit.*

Mapa 4. Distribución geográfica de los cables revelados por *WikiLeaks*



Fuente: *Perfil.com,* sección "El Observador", 4 de diciembre de 2010, p.3.

Respecto a las reacciones generadas mientras algunos líderes estatales se sumaban al reclamo internacional en torno a la forma en la que se expresaban los funcionarios estadounidenses de determinadas regiones y personajes políticos, otros sostenían que las filtraciones no hacían más que confirmar lo que ya suponían. Sin embargo, así como hubo naciones donde el acontecimiento paso inadvertido, también existieron casos donde la publicación provocó que representantes diplomáticos abandonaran sus funciones.

Mientras las filtraciones recorrían el globo a través de la *Word Wide Web* la sociedad también formaba parte del conflicto, diversos ciudadanos de todas partes del mundo conocieron del tipo de relación que su país tenía con Washington. El impacto generado en la población al colocar a su alcance, por primera vez, documentos oficiales sobre las relaciones exteriores de prácticamente todas las naciones, fue tal que algunos gobiernos optaron por bloquear el acceso a *WikiLeaks* e incluso prohibir el tema en foros de discusión y blogs nacionales.[123]

La prensa dedicó encabezados durante semanas al contenido de las filtraciones mientras representantes de Estados Unidos en distintos países ofrecieron conferencias de prensa

[123] Democracy Now. (Diciembre 12, 2010) "¡Qué democracia!: Departamento de Estado prohíbe WikiLeaks a personal y amenaza a estudiantes que los citen". *Aporrea*. [En línea] Disponible en: <http://www.aporrea.org/tiburon/n170786.html>. (Consulta 26/04/2013).

condenando la filtración y abogando por mantener intactas las relaciones diplomáticas de su país con el resto del mundo.

En América Latina en general las reacciones fueron moderadas —salvo algunos casos como como Venezuela, Ecuador y Cuba cuyas reacciones en contra de la política exterior estadounidense fueron más agresivas e incluso Ecuador expulsó a la representante de EE.UU. de su territorio[124]—. En el caso de Venezuela, por ejemplo, el entonces presidente Hugo Chávez solicitó la renuncia de la Secretaria de Estado Hillary Clinton y acusó a Estados Unidos de cometer espionaje,[125] mientras que por otro lado el gobierno colombiano se solidarizaba con Washington. En el plano nacional la respuesta del entonces Presidente Felipe Calderón Hinojosa fue que quienes habían escrito los cables exageraron la situación de México respecto a la lucha contra el narcotráfico, y aunque el embajador en turno, Carlos Pascual, presentó su renuncia poco después, la relación entre Estados Unidos y México no sufrió consecuencias graves.[126]

En Medio Oriente Daoud Sultano y, miembro del parlamento afgano, declaró en una entrevista para *RT* que los cables exponían conjeturas hechas por los representantes de Washington, opiniones similares a rumores, y que se estaba exagerando el asunto con el fin de otorgarle tintes políticos.[127] En Israel el primer ministro Binyamin Netanyahu, expresó que lo único negativo en las publicaciones era las observaciones que diplomáticos estadounidenses hicieron respecto a figuras políticas de distintos países, y que prácticamente su país (Israel) no fue perjudicado, sino al contrario, que los cables apoyaban su noción sobre la grave amenaza que representa Irán para la región y el resto del mundo.[128]

---

[124] Assange, Julian. "Diálogos con Assange". *RT*, capítulo 6. [En línea]. Disponible en: <http://assange.rt.com/es/el-mundo-delmaana-episodio-5-assange-y-correa-la-esperada-entrevista-en-rt/full-translation-text/#page-1>. (Consulta 03/07/2013).

[125] "WikiLeaks dejó al imperio al desnudo, dice el presidente Hugo Chávez". (Noviembre 30, 2010). *CNN México*. [En línea]. Disponible en: <http://mexico.cnn.com/mundo/2010/11/30/wikileaks-dejo-al-imperio-al-desnudo-dice-elpresidente-hugo-chavez>. (Consulta 20/06/2013).

[126] "Renuncia de Carlos Pascual fue 'decisión personal': EU". (Marzo 22, 2011). *La Jornada*. [En línea]. Disponible en: <http://www.jornada.unam.mx/2011/03/22/politica/006n1pol>. (Consulta 02/02/2013).

[127] "Los informes clasificados de Wikileaks despiertan a Amnistía Internacional". (Julio 27, 2010). *RT*. [En línea]. Disponible en: <http://actualidad.rt.com/video/actualidad/view/70643-Los-informes-clasificados-de-Wikileaks-despiertan-a-Amnist%C3%ADa-Internacional>. (Consulta 12/05/2013).

[128] Kaplan, Rubén. "Wikileaks y Medio Oriente". *ANAJNU*. [En línea]. Disponible en: <http://www.anajnu.cl/wikimedioooriente.htm>. (Consulta 2/06/2013).

De parte de los representantes de Islamabad (Paquistán) el Ministro de exterior Abdul Basit consideró que documentos tan importantes no debían publicarse. Mientras que en la República de la India la Ministro de asuntos exteriores Praneet Kaur optó por mantenerse al margen de lo que consideró un asunto delicado.[129]

Por otra lado, entre las reacciones más distintivas figura: Líbano, cuyos diplomáticos declararon que el objetivo de *WikiLeaks* era generar un disturbio en la nación debido al contenido de las publicaciones; para Hosein Yilick Vicepresidente del Partido de justicia y desarrollo turco probablemente Israel estaba involucrado en dichas revelaciones con el fin de alcanzar objetivos políticos internos y externos; Iyad Alawi ex Primer ministro iraquí señaló que el objetivo de las publicaciones era aumentar las tensiones en la región; Franco Feratini Ministro de exteriores italiano expresó que *WikiLeaks* representaba el 11-S de la diplomacia estadounidense, y en Iraq el Ministro de exteriores indicó que la organización de Assange perjudicaba de forma considerable las relaciones internacionales.[130]

A pesar de que la mayor parte de los diplomáticos respondió con prudencia, la magnitud de las revelaciones provocó que la Secretaria de Estado Hilary Clinton convocara el 31 de enero de 2011 una reunión de más de doscientos representantes estadounidenses para tratar el tema.[131]

Por parte de la sociedad el debate fue todavía más diverso, pues no sólo se limitaba a apoyar o condenar las filtraciones, sino que la mayor parte de la atención se centró en su contenido. Ciudadanos de distintas partes del mundo no sólo podían acceder libremente a la información filtrada sino que eran capaces de compartirla con otros usuarios, creando foros de discusión o publicando entradas en cientos de blogs. Fue la primera vez que la sociedad formó parte de un intercambio mundial de datos en torno a un mismo tema —pues por todas partes del globo cientos de activistas crearon sitios "espejo" que aseguraban el acceso al

---

[129] "Reacciones ante destape de Wikileaks". (Noviembre 29, 2010). *Perú 21*. [En línea]. Disponible en: <http://peru21.pe/noticia/676471/reacciones-ante-destape-wikileaks>. (Consulta 02/05/2013).

[130] "Reacciones a las revelaciones de Wikileaks". (Diciembre 6, 2010). *Irán Spanish Radio*. [En línea]. Disponible en: <http://spanish.irib.ir/an%C3%A1lisis/art%C3%ADculos/item/110023-reacciones-a-las-revelaciones-de-wikileaks>. (Consulta 26/06/2013).

[131] "Convocan a reunión masiva de embajadores de EU; Egipto y WikiLeaks, causas". (Febrero 1, 2011). *Criterio Hidalgo*. [En línea]. Disponible en: <http://www.criteriohidalgo.com/notas.asp?id=36152>. (Consulta 24/05/2013).

material, debido a las medidas restrictivas que adoptó la mayoría de las naciones— generando un debate de alcance internacional.

Las redes sociales sirvieron como catalizador para discutir lo que, desde distintos puntos de de vista, parecía un suceso sin precedentes. En *Twitter* y *Facebook* inmediatamente surgieron surgieron intentos para censurar el tema; sin embargo, dichas medidas sólo consiguieron impulsar la temática. El impacto de las publicaciones en las redes sociales se refleja en la cuenta de *WikiLeaks* en *Twitter* que pasó de tener 522 000 seguidores el 10 de diciembre de 2010,[132] a 2 235 651 el 9 de mayo de 2014.

La comunidad *hacktivista* en las redes sociales manifestó su apoyo a Julian Assange y a la organización, en especial el grupo hacker *Anonymous*.[133] Por otro lado estaban los que consideraron que *WikiLeaks* constituía una amenaza para la seguridad internacional.

El fenómeno generó diversas reacciones e independientemente de las posturas, se convirtió en tema central en los medios de comunicación durante semanas; suscitó debates en los círculos políticos de todo el mundo, y la ciudadanía formó parte activa de esa discusión. La esfera política internacional parecía despertar crudamente a la nueva realidad diplomática, caracterizada por nuevas herramientas, nuevos actores, nuevos canales de interconexión; pero también de nuevas necesidades, desafíos y amenazas. El ambiente diplomático contemporáneo presenta nuevos retos pero también nuevas oportunidades, aspecto que coincide con la opinión del profesor de la Universitat Oberta de Catalunya, Manuel Castells sobre que:

> […] *Internet puede permitir la desburocratización de la política y superar la crisis de legitimidad de los gobiernos que se produce en todo el mundo, a partir de una mayor participación ciudadana permanente, interactiva, y a una información constante de doble vía.*[134]

---

[132] Cuen, David. (Diciembre 10, 2010). "WikiLeaks: denuncian censura en las redes sociales". *BBC*. [En línea]. Disponible en: <http://www.bbc.co.uk/mundo/noticias/2010/12/101213_1112_wikileaks_twitter_redes_sociales_facebook_algoritmo_dc.shtml>. (Consulta 24/05/2013).

[133] *Ídem.*

[134] Castells, Manuel. *Lliçó inaugural del programa de doctorat sobre la societat de la informació i el coneixement*. Universitat Oberta de Catalunya. [En línea]. Disponible en: <http://www.uoc.edu/web/cat/articles/castells/print.html>. (Consulta 26/06/2013).

3.6. Consecuencias de las publicaciones

A continuación se abordarán los cambios generados en el ámbito político, social, periodístico y diplomático, y se analizará el panorama de las relaciones entre Estados, tras la controversia *WikiLeaks*.

La totalidad de repercusiones entorno a la publicación de cables diplomáticos es difícil de conocer; las consecuencias inmediatas fueron evidentes, una serie de reclamos y protestas respecto a la forma en la que Washington se expresó de ciertas figuras políticas, así como del alcance de sus funciones dentro de los países u organismos anfitriones, sin embargo las consecuencias a largo plazo serán más profundas. En el terreno político surgen nuevos actores y nuevas formas de interacción ciudadana, que reflejan la transformación del escenario nacional e internacional, así como la necesidad de establecer medidas capaces de proteger y regular el intercambio mundial información; la práctica política deberá adecuarse a un entorno diferente, a fin de cumplir eficientemente que con sus objetivos.

El impacto generado en la sociedad nacional e internacional será quizá el más difícil de calcular; los nuevos medios han demostrado sus alcances a favor de la libertad de información y la transparencia; en este sentido todavía se está muy lejos de conocer las repercusiones generadas por *WikiLeaks*. El presente análisis se desarrolla en el marco de una nueva filtración de información confidencial perteneciente al gobierno estadounidense, llevada a cabo —una vez más— por un miembro de la estructura militar y de inteligencia norteamericana —anteriormente Bradley Manning, ex analista militar, entregó miles cables diplomáticos y otros documentos clasificados a *WikiLeaks*[135]—. Edward Joseph Snowden ex consultor de inteligencia, ante las prácticas de ciberespionaje llevadas a cabo por su gobierno, Estados Unidos, decidió denunciarlos públicamente a través de los medios internacionales en junio de 2013, y al hacerlo rechazó el anonimato.[136] Es necesario mencionar este caso, pues pareciera que el fenómeno *WikiLeaks* ha dejado tras de sí una estela profunda e inescrutable en la consciencia social. Por otro lado es interesante observar

[135] Soldado y analista militar que proporcionó documentos clasificados a WikiLeaks, referentes a las operaciones militares y actividades diplomáticas del gobierno estadounidense.

[136] "Con 4 notebooks, una llave USB y un cubo Rubik, Snowden destapó cómo funciona el espionaje mundial" (Julio 1, 2013) *iprofesional*. [En línea]. Disponible en: <http://www.iprofesional.com/notas/164134-Con-4-notebooks-una-llave-USB-y-un-cubo-Rubik-Snowden-destap-cmo-funciona-el-espionaje-mundial>. (Consulta 20/07/2013).

que los Estados deban protegerse de sus propios ciudadanos (Manning y Snowden), la causa —sin duda— son los delitos cometidos en contra de la privacidad, la libre expresión, el derecho derecho a la información, y la violación de los principios que rigen el Derecho Internacional. El El caso Snowden apareció el 7 de junio de 2013, y con ello, lo que muchos medios han clasificado como una nueva crisis diplomática para Estados Unidos, pues el ex analista dio conocer mecanismos de ciberespionaje en contra de embajadas de por lo menos 38 naciones.[137] La atención parece orientarse no tanto a la violación de la confidencialidad de las operaciones gubernamentales sino al alcance de éstas, pues trastocan la ilegalidad. Diplomáticos de todo el mundo piden explicaciones a Washington, mientras que diversos periódicos revelan que la administración Obama vigiló incluso a sus aliados. Al mismo tiempo líderes europeos señalaron que es necesario que Estados Unidos reestablezca la confianza en sus relaciones.[138]

Existen muchas voces que condenan a Snowden, pero las actividades ilícitas del gobierno estadounidense no sólo involucraban la intercepción de comunicaciones a líderes políticos, también las de sus ciudadanos; como respuesta tanto la sociedad estadounidense como la del resto del mundo demandan mayor transparencia en los mecanismos de seguridad de su propia nación. La comunidad diplomática internacional se ha dado cuenta de la importancia de proteger las comunicaciones oficiales; no se trata de una nueva Guerra Fría, caracterizada por la competencia constante entre espías, sino de renovar aquel elemento que es esencial y que ha regido las relaciones entre los Estados a través de la historia: la confianza mutua y el respeto a las normas internacionales.

Es preciso señalar que el alcance de *WikiLeaks* y del caso Snowden en la sociedad internacional se debió, en buena medida, al desconocimiento de la ciudadanía en los asuntos fundamentales de su propia nación. Si bien existen datos que por su naturaleza deben mantenerse en confidencialidad, la sociedad contemporánea demanda, día a día, mayor participación en los asuntos de su país, por consecuencia resulta imperioso establecer mecanismos de interacción gobierno-sociedad más incluyentes y transparentes. Por otro lado a pesar de que existen opiniones a favor y en contra de las filtraciones es innegable que las comunicaciones oficiales poseen un carácter esencial en el ámbito económico, político y

[137] Pérez Silva, Ciro. (Julio 2, 2013). "México trata de manera directa con EU las 'presuntas filtraciones': SRE". *La Jornada*, p. 3.
[138] "John Kerry alega que 'no es inusual' buscar información de otros países". (Julio 2, 2013). *La Jornada*, p.3

diplomático de una nación y cualquier uso indebido es capaz de poner en riesgo la seguridad de todo un continente.

En el ámbito social quedó demostrado el alcance de las nuevas tecnologías a favor de la transparencia y la democracia; el uso del ciberespacio como un canal eficaz para la comunicación entre habitantes de todas partes del mundo, especialmente cómo una vía eficaz para denunciar aquello que resulta inconveniente para las autoridades nacionales, y al mismo tiempo lleva a considerar a las TIC e Internet como una herramienta poderosa, capaz de colocar al alcance de todos una cantidad de información como nunca antes en la historia. No obstante, nuevas formas de convivencia representan también nuevos desafíos, a la par de conceptos como "Era tecnológica" y "Sociedad de la información" reaparecen otros como "irrupción ilegal" y "sustracción ilícita". Situación que sólo puede verse opacada por el surgimiento de una nueva sociedad más informada y participativa que sin duda ocupará un lugar importante a la hora de fijar medidas orientadas a la regulación del *Word Wide Web*.

En la esfera periodística el trabajo profesional ha sido reivindicado, pues la enorme cantidad de datos con los que deben trabajar los periodistas de hoy día es impresionante. La variedad de formatos y herramientas de trabajo complican la labor periodística, y al mismo tiempo la enriquecen.

En el plano internacional, entre las consecuencias inmediatas, está la reconfiguración de las relaciones entre Estados, de forma particular con aquellas naciones donde las revelaciones afectaron considerablemente los vínculos diplomáticos con Washington, aunque la mayoría de los representantes adoptó una posición moderada al respecto y se solidarizaron con Estados Unidos ante la publicación de observaciones que —según su opinión— cualquier funcionario exterior pudo haber hecho de otras naciones. Sin embargo, más allá de la reacción entre homólogos, lo más importante fueron aquellas negociaciones que se vieron afectadas por las revelaciones. Es preciso recordar que las comunicaciones diplomáticas entre los países se relacionan con diferentes ámbitos como el político, militar, económico, etc. Por lo que resulta imposible determinar cuáles serán las consecuencias a largo plazo; lo que sí está claro es que a partir de las publicaciones Estados Unidos y el resto de los países implementarán medidas para la regulación del ciberespacio. Sin duda, el ambiente diplomático tradicional fue alterado, pero lejos de abandonar el uso de las TIC

como canal diplomático oficial o evitar la transcripción de los asuntos tratados en reuniones entre autoridades, lo que se debe procurar es la protección eficiente de las comunicaciones oficiales y establecer mecanismos más eficaces de transparencia y de comunicación con la ciudadanía.

Con el fenómeno *WikiLeaks* fue posible percibir de forma significativa un cambio en la realidad nacional e internacional, impulsado en buena medida, por nuevas formas de convivencia. En cuanto dicha transición, y abordando el plano diplomático, el académico Thomas Nowotny (2011) docente de la Universidad de Viena, advierte la reconfiguración de la arena mundial. Nowotny establece tres cambios importantes con la arribo de la Era tecnológica: el primero es el carácter público y global de una pieza clave para la política: la información; el segundo es el incremento en el peso de la opinión pública, gracias al aumento de gobiernos democráticos, y el tercero el surgimiento de nuevos actores no gubernamentales. Nowotny también plantea que la actividad diplomática convencional no está del todo preparada para enfrentarse a la nueva realidad internacional, por lo que es necesario que los servicios diplomáticos se adapten cuanto antes a su nuevo entorno; señala que han surgido nuevas tareas, y en consecuencia se necesitan nuevas herramientas, y que tanto instituciones como métodos de trabajo deben transformarse para responder a las exigencias de la Era informática.

3.7. Los nuevos retos para el periodismo tradicional

La revolución telemática ha logrado influir en diferentes campos desde la medicina, las artes, la economía, la política, la ciencia y, como se ha observado, la diplomacia. Este fenómeno también ha transformado el ejercicio periodístico de forma gradual, por lo que tanto editoriales como corresponsales se enfrentan a un nuevo ambiente informático; al mismo tiempo la demanda por parte de la sociedad también ha cambiado. El periodista ha adoptado nuevas prácticas para la búsqueda, construcción, edición y presentación de su trabajo, mientras tanto las editoriales han incursionado en nuevas áreas, ampliando su presencia en redes sociales, probando aplicaciones tecnológicas, adoptando nuevas modalidades de subscripción, etc. Si bien Internet les ofrece mayor proyección también las coloca en un mercado en donde el número de competidores es considerablemente superior.

En la actualidad la sociedad necesita medios de comunicación confiables y competentes, ya que el flujo de información ha aumentado drásticamente con la llegada de las innovaciones tecnológicas. Hoy día el público se enfrenta a una gran cantidad de datos disponibles en distintos medios como blogs, agencias de noticias, portales web, redes sociales, aplicaciones móviles, etc. La práctica periodística tradicional lejos de quedar obsoleta, hoy más que nunca es esencial.

Antes de la difusión de las TIC los medios informáticos afrontaban el problema de la escasez de datos, el periodismo —y en especial el periodismo de investigación— representaba un verdadero desafío, había que consultar diferentes fuentes, incluso viajar largas distancias y se precisaba de un largo proceso de investigación. Hoy en día miles de portales en todo mundo comparten cientos de datos en la web, las agencias de noticias proporcionan información que renuevan a cada segundo de forma que la práctica periodística parece medirse en bits por segundo. Antes de continuar analizando el efecto delas nuevas tecnologías en el ámbito periodístico actual, vale la pena hacer una breve revisión sobre su evolución histórica respecto al procesamiento y transmisión de información.

Desde sus inicios los ordenadores ya demostraban un amplio potencial comunicativo. Joseph Carl Robnett Licklider y Robert W. Taylor, pioneros del desarrollo computacional, declaraban que los ordenadores se convertirían en una importante vía de conexión para millones de personas alrededor del mundo.[139]Aunque en un principio los ordenadores personales no fueron concebidos como herramientas de comunicación, poco a poco, diversos investigadores dedicaron gran parte de su tiempo a explorar ese aspecto. En 1960 Licklider escribió *Man-computer Symbiosis* donde describe una especie de asociación entre hombres y maquinas; según Licklider el hombre fijará objetivos, formulará hipótesis, determinará criterios y llevará a cabo evaluaciones mientras que las maquinas harán el trabajo de rutina, preparando el camino para que el pensamiento científico pueda encargarse de interpretar y resolver situaciones.[140] Poco después en 1968 Licklider y Robert Taylor (entonces director de Información del *Information Processing Techniques Office* de ARPA) publicaron un

[139] Hacker, Kenneth y Jon Van Dijk. (2000). *Digital Democracy. Issues of Theory and Practice*. Reino Unido: SAGE.
[140] Robnett Licklider, Joseph Carl. (Marzo, 1960). *Man-Computer Symbiosis*. IRE Transactions on Human Factors in Electronics, volumen HFE-1, pp. 4-11. [En línea]. Disponible en: <http://sloan.stanford.edu/mousesite/Secondary /Licklider.pdfer.html>. (Consulta 12/02/2013).

estudio revolucionario para su época y que ya dejaba entrever el enorme potencial de los equipos de cómputo, se trata de *The Computer as a Communication Device*[141] donde establecen establecen que los avances científicos y tecnológicos serían capaces de enlazar individuos de distintas partes del mundo. También señalan la transición hacia una Era tecnológica donde lejos lejos de recibir y enviar información, el usuario sería capaz de interactuar con las nuevas herramientas. En este estudio Licklider y Taylor establecen que: "se trata de algo más que la transferencia en un solo sentido"[142] y que los ordenadores trasformarían las formas de comunicación e interacción humana. Desde finales de los sesenta el Departamento de Defensa de Estados Unidos creó la Agencia de Proyectos de Investigación Avanzados, DARPA (por sus siglas en inglés), con el fin de construir un sistema de comunicación flexible y dinámico entre ordenadores, posteriormente surgió Arpa-Net (una red de computadoras del *Advanced Research Projects Agency Network*) que logró enlazar 4 ordenadores ubicados en distintos lugares. Para 1980 el modelo Arpa-Net ya contaba con 100 equipos de cómputo interconectados.[143] Siguiendo esta línea en 1984 la compañía *Digital Equipment Corporation* fundó el *Systems Research Center*[144] con el objetivo de mejorar el conocimiento y las técnicas de los sistemas informáticos; en 1990 Tim Berners-Lee realizó un gran aporte para la interconexión global e intercambio de datos, desarrolló el *Word Wide Web* que sin duda alguna sentó las bases de lo que hoy día se conoce como *aldea global.*[145] A partir de este momento la cantidad de interconexiones incrementó paulatinamente alrededor del mundo. Poco a poco, surgieron nuevos medios de interconexión y de transferencia de datos aunque en un principio se limitaban solo a caracteres textuales poco a poco incorporaron documentos, imágenes, sonidos y videos.

Con el siglo XXI llegó también lo que muchos estudiosos han denominado la "Era tecnológica" donde el desarrollo de las ciencias y sus aplicaciones transformaron de manera

---

[141] Hacker, Kenneth. *Óp. Cit.*

[142] Robnett Licklider, Joseph Carl y Robert W. Taylor. (Abril, 1968). *The Computer as a Communication Device*. Science and Technology. [En línea]. Disponible en: <http://sloan.stanford.edu/mousesite/Secondary/Licklider.p>. (Consulta 12/02/2013).

[143] Flores Vivar, Jesús. (2010). *Ciberperiodismo: nuevos enfoques, conceptos y profesiones emergentes en el mundo infodigital*. México: Limusa.

[144] *Ídem.*

[145] Marshall Mc Luhan introdujo este concepto, refiriéndose a un nuevo modelo de sociedad.

importante la forma de vida de muchos individuos, y consecuentemente modificaron la práctica y estudio de distintas disciplinas, entre ellas la práctica periodística.

Existe un debate en torno a si Internet y las TIC han llegado o no a revolucionar el periodismo y los medios de comunicación. Según Roger Fidler (1998) se está pasando por *mediamorfosis* en donde la práctica periodística ha ido adoptando nuevas funciones.

En este sentido el periodista enfrenta también nuevos desafíos, pues se encuentra en un nuevo escenario caracterizado por: mayor número de usuarios, información generalizada y el incremento de bases de datos o información dura; por lo que es necesario dedicar más tiempo al análisis y procesamiento de datos. Han surgido también diversas fuentes y tipos de información, y diferentes clases de público.[146] Por esta razón la información debe ser clara y concisa, aunado a esto la diversidad de lenguajes ha obligado a que muchas agencias informativas traduzcan sus portales web a más de un idioma. En síntesis la información —materia prima de los medios de comunicación— se ha transformado. Actualmente los datos pueden ser presentados en múltiples plataformas (audio, video, fotografías, gráficas, diagramas interactivos, etc.), además se ha dado una diversificación ya que hoy en día el investigador puede acceder al sitio oficial de secretarías, departamentos de Estado o ministerios; centros de investigación, institutos y organismos internacionales o especializados para solicitar datos, reportes, estadísticas, estudios, documentos, etc. sin viajar largas distancias.

En cuanto a la necesidad de nuevas habilidades por parte del periodista, es posible mencionar el uso de nuevas herramientas como los motores de búsqueda. Este tipo de herramientas refuerzan el ejercicio periodístico, facilitando la tarea del corresponsal. Sin embargo, tuvieron que pasar varios años para conseguir programas tan sofisticados como los de hoy en día. Otros instrumentos son los foros de discusión que sirven para difundir noticias que sin duda colaboran a la publicidad de las agencias noticiosas.

Por otra parte, el *Word Wide Web* permite crear documentos de hipertexto con enlaces a sitios de referencia o consulta, brindar soporte técnico al usuario, incorporar imágenes y sonido, y elaborar presentaciones interactivas. Por último las redes sociales hoy en día

[146] Flores Vivar. *Óp. Cit.*

poseen un lugar central, pues sirven de enlace directo, estableciendo una comunicación constante con la audiencia.[147]

Según Jesús Flores Vivar (2010) doctor en ciencias de la información en la Universidad Complutense de Madrid, las innovaciones tecnológicas han repercutido en dos formas en el ámbito periodístico: en el proceso y en el producto.

En otro orden de ideas, el incremento en el flujo de información demanda mayor dedicación por parte del periodista, pues han surgido diferentes portales especializados en diferentes temáticas, que representan un aumento en la competencia periodística; además hoy día el usuario demanda mayor interacción con el corresponsal, pues actualmente es capaz establecer comunicación directa a través de las redes sociales e incluso comentar las notas.

Las posiciones respecto al uso de la TIC en el periodismo son diversas, por un lado están quienes se oponen y señalan que han surgido cientos de sitios web que en realidad no ejercen periodismo; que cada vez se presta más atención al formato y no al contenido de las notas; que la investigación periodística ha perdido su dinamismo, y que se le ha restado importancia a la credibilidad de las fuentes, desde este punto de vista, el valor de un artículo debe determinarse por el uso de fuentes serias y confiables.

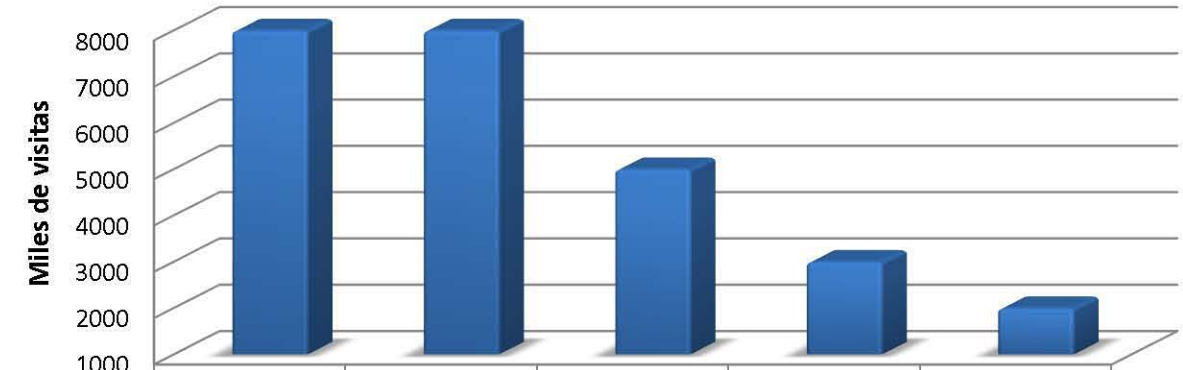
Por otro lado, están quienes apoyan el uso de nuevas herramientas y sostienen que la revolución telemática no desplaza la práctica periodística tradicional sino que la complementa, pues hoy día las agencias de noticias son capaces de enriquecer sus notas con archivos de audio y video; integrar a la audiencia en sus publicaciones (por medio de foros, encuestas, calificación de notas, etc.); estar disponibles en prácticamente cualquier lugar; intercambiar información forma rápida con corresponsales en todas partes del mundo; remitir a los documentos originales que se toman como referencia, y dar diversos formatos a la presentación de sus artículos. A pesar de la diversidad de opiniones algo que es indudable es que la globalización de la información ha incrementado la necesidad de un periodismo crítico y objetivo.

Además, el uso de Internet como medio de información y comunicación ha aumentado de forma considerable en los últimos años. Según cifras de la Unión Internacional de

[147] *Ídem*

Telecomunicaciones a finales de 2013 el 40% de la población mundial contaba con acceso a la red,[148] por lo que el impacto de las plataformas tecnológicas en la práctica periodística es considerable. Según Teqpad —una herramienta calificadora de páginas web— el diario estadounidense *The New York Times* recibe unas 7 913 669 visitas por día, mientras que en México el periódico *La Jornada* recibe aproximadamente 590 445 visitas diarias[149] (véase gráficas 3 y 4). Las repercusiones de la innovación tecnológica son evidentes en muchas áreas y el ejercicio periodístico no es una excepción. No obstante sus principios y funciones básicas continúan vigentes: informar objetivamente del acontecer nacional e internacional, pues en la Era informática la práctica periodística debe enfrentar nuevos desafíos y aprovechar al máximo las ventajas.

Gráfica 3. Periódicos internacionales en línea más visitados



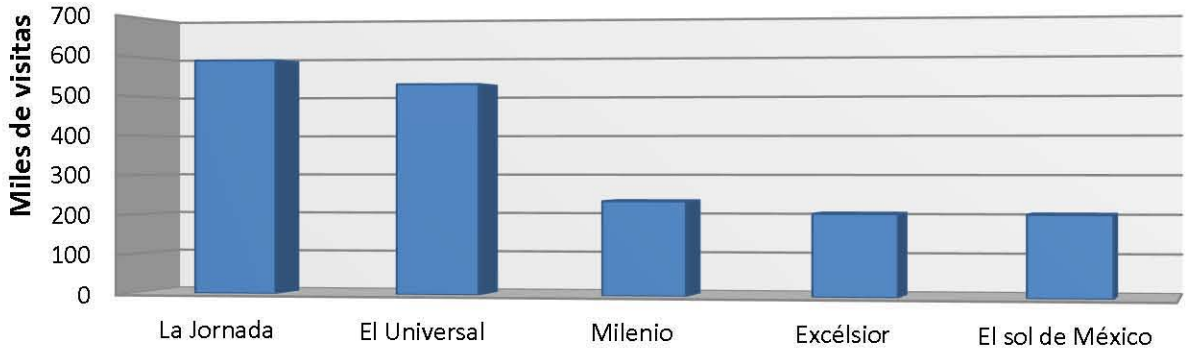
	The New York Times	The Daily Mail	The Guardian	The Washington Post	El País
visitas por día	8000	8000	5000	3000	2000

Fuente: Elaboración propia con datos obtenidos de <www.teqpad.com> al 2 de julio de 2013.

[148] *La UIT publica las cifras técnicas y clasificaciones mundiales más recientes*. (Octubre 7, 2013). Ginebra, Suiza. [En línea]. Disponible en: <http://www.itu.int/net/pressoffice/press_releases/2013/41-es.aspx#.U261OoF5PHo>. (Consulta 10/05/2014).

[149] Datos recolectados al 1° de junio de 2013, Teqpad. [En línea]. Disponible en: <http://www.teqpad.com>.

Gráfica 4. Periódicos nacionales en línea más visitados



	La Jornada	El Universal	Milenio	Excélsior	El sol de México
visitas por día	590	528	236	206	205

Fuente: Elaboración propia con datos obtenidos de <www.teqpad.com> al 2 de julio de

3.8. Las nuevas tecnologías y los movimientos sociales

Las agrupaciones sociales constituyen un elemento importante para la democracia, sin duda alguna sus acciones repercuten en los ámbitos político y económico, tanto a nivel nacional como internacional. Por ello es necesario analizar ¿cuál ha sido su transformación? y ¿cuáles son las ventajas y desventajas que representa el uso de las TIC en los movimientos sociales?

La innovación tecnológica ha optimizado el entorno y la práctica de la acción ciudadana. La red es una herramienta organizativa y además un importante instrumento de comunicación. Cada día grupos activistas, organismos internacionales, asociaciones civiles y ONG utilizan Internet como canal de comunicación, ya que es capaz de conectarlos en tiempo real con distintas partes del mundo, además les permite intercambiar diferentes tipos de datos, en grandes cantidades y en cuestión de segundos.

La web constituye un vehículo para divulgar ideas, iniciativas, proyectos y demandas sociales a nivel mundial. Por lo tanto la capacidad acción de agrupaciones civiles en el siglo XXI es mayor. De forma que si las autoridades permanecen indiferentes ante determinada situación, la sociedad puede exponer el caso a la comunidad internacional mediante el uso de nuevas tecnologías; como consecuencia diferentes entidades toman una posición activa al respecto y demandan su resolución, incrementando así la presión internacional en el tema.

En este sentido los movimientos sociales pueden afectar la imagen pública de entidades financieras, figuras políticas, funcionarios, organizaciones e incluso la de Estados, por consiguiente logran influir también en la interacción diplomática de las naciones. Se trata del empoderamiento de un antiguo actor, con el que los Estados y demás entidades mundiales tendrán que aprender a interactuar. Hoy día en comparación con épocas anteriores las agrupaciones civiles difícilmente pueden ser silenciadas, la red de redes les proporciona un espacio para comunicarle al mundo sus objetivos e incluso para cooperar con organizaciones internacionales.

El uso de las TIC en los movimientos sociales es un asunto que plantea ventajas y desventajas entre las primeras está que en la actualidad los grupos disidentes cuentan con herramientas más eficientes para promocionar su causa, y al mismo tiempo comparten con el mundo la forma en la que sus gobernantes manejan determinada situación a través de reportes, videos, audios, fotografías, testimonios, etc., que en cuestión de segundos están al alcance de todos. Otro aspecto positivo es que en el plano nacional diversos actores han conseguido proyección mundial gracias al ciberespacio; estas entidades demandan soluciones por de parte de las autoridades nacionales, incrementando la presión internacional. De este modo los movimientos sociales ayudan a denunciarla ausencia de derechos humanos; exigen transparencia y democracia, y también evidencian casos de corrupción e impunidad. Por otra parte dichas organizaciones también están al tanto de la actividad diplomática de sus países y son capaces de fijar posturas sobre determinados temas e incluso pueden oponerse abiertamente a alguna resolución. En cierta forma representan la voz de la ciudadanía, aunque no de su totalidad. Por lo tanto, inevitablemente, tanto dirigentes nacionales como representantes diplomáticos están conscientes de que cada una de sus decisiones será sometida a un fuerte análisis por parte de estas agrupaciones.

Bajo esta misma línea, según Ted Koppel (periodista británico), parece que se ha consolidado la teoría acerca de que la revolución telemática ha fortalecido a las entidades no estatales. Pues hoy en día son capaces de desafiar la autoridad de quienes están en el poder.[150] Cada lucha o movimiento puede ser conocido por el mundo entero, transformando

[150] *Redes y guerras en red: el futuro del terrorismo, el crimen organizado y el activismo político*. (2003). Madrid: Alianza, p. 158. Citado por Tiffany Danitz.

la percepción que los otros Estados tienen de un país, con ello incrementan la labor de los representantes diplomáticos, y diversifican el número de actores en la escena mundial.

Sin embargo, no todo es positivo conscientes del potencial de las nuevas herramientas telemáticas algunos gobiernos han decidido restringir el acceso a la red —China, Cuba, Corea del Norte, Irán, Vietnam, entre otros— en estos casos las barreras físicas y virtuales siguen dominando la aldea global. De la misma forma diversos regímenes que permiten el acceso al ciberespacio han tratado de controlarlo e incluso manipularlo. Este punto ha logrado confrontar opiniones en torno a si el ciberespacio necesita o no ser regulado. Por un lado, se presentan quienes defienden el derecho a la privacidad y al libre flujo de información; por el otro, los que afirman que es necesario utilizar todos los medios para asegurar la estabilidad política y social, y con ello el bienestar nacional.

Existen diversos teóricos que conciben la innovación telemática como un beneficio para la sociedad —Lévy, *Ciberdemocracia, Ensayo sobre filosofía política* (2004); Dertouzos *Redes como naciones* (1997); Lipnack y Stamps, *La era de las redes* (1994), y Castells y Kumon *Sociedad Red* (1992)[151]—, pero también están los que mantienen una posición distinta, como Johanna Neumann, quien señala: "cuando un sistema político absorbe una nueva tecnología, el público puede experimentar un aumento temporal en su influencia, antes de que el equilibro de poder vuelva a su situación de partida de custodia compartida".[152] Respecto a la democracia y las nuevas tecnologías, David Ronfeldt doctor en ciencia política, afirma: "la *cyberocracia* [transformación tecnológica de la democracia] lejos de favorecer a la democracia o al totalitarismo puede hacer posible formas más avanzadas, más opuestas y más alejadas de ambas".[153]

Por otra parte, una desventaja respecto a la relación nuevas tecnologías-movimientos sociales es que el acceso a las TIC no es generalizado, pues en los países en vía de desarrollo —y que generalmente se ven más afectados por cuestiones como pobreza, corrupción y represión— el acceso a Internet es complicado, de manera que existe una especie de

[151] *Ídem.* p. 333
[152] *Ídem.,* p. 159.
[153] *Ídem.,* p. 160.

discriminación tecnológica,[154] puesto que la capacidad de actuar, la información y el contacto con organizaciones a favor del bienestar social están condicionadas al acceso a estas herramientas (véase gráfica 5).

Gráfica 5. Número de personas con acceso a Internet en el mundo por países (de acuerdo a nivel de desarrollo) 2007-2014

***Datos estimados**

Fuente: International Telecommunication Union. *The World in 2014: ICT Facts and Figures*. (Abril, 2014), p.1.

Otro aspecto negativo es el hecho de que personas fuera del país puedan promover, organizar o apoyar una "causa" nacional a través de la red, pues no siempre puede ser en beneficio de la sociedad, dado podría funcionar como instrumento de desestabilización a favor de intereses alejados del bienestar común.

Es preciso señalar que el ciberespacio requiere como cualquier otra forma de interacción social de normas que regulen sus funciones, no en el sentido de represión y control, sino con el fin de asegurar la interacción equilibrada de todos los miembros y el respeto a sus derechos. En relación con esto resulta complicado establecer una posición, dado que las comunicaciones continúan evolucionando y con ello la sociedad misma. Por otra parte a pesar de la constante evolución de las comunicaciones todavía existen lugares en donde conceptos como "Tecnologías de la Información y la Comunicación", "derecho a la información", "transparencia institucional" y "ciberactivismo", entre otros, son completamente desconocidos; por ejemplo en África Subsahariana hay menos de una línea

[154] *Ídem.*

de teléfono fija por cada 100 habitantes, y en el sur de Asia el 42% de los poblados carece de servicio telefónico.[155]

En síntesis el uso de las nuevas tecnologías, específicamente la red, en los movimientos sociales posee pros y contras (véase tabla 5) todo depende de la forma en la que se usen.

Tabla 5. Las TIC y los movimientos sociales

Uso de nuevas tecnologías en los movimientos sociales	
VENTAJAS	• La web es económica y cómoda • Es una herramienta organizativa • Coloca la información al alcance de los dirigentes del movimiento de forma rápida y segura • Permite a los seguidores seleccionar su nivel de actividad • Da publicidad a la causa o campaña • Otorga ventajas sobre quienes no utilizan nuevas tecnologías
DESVENTAJAS	• Es riesgoso tomarla como único medio de confirmación • Las comunicaciones pueden ser interceptadas • Los portales pueden sufrir sabotaje • Dado que no existe un mediador, carecen de confianza • Divide a quienes tienes acceso a ellas y quienes no • No puede reemplazar al contacto humano en el *lobby* y en otras actividades de difusión

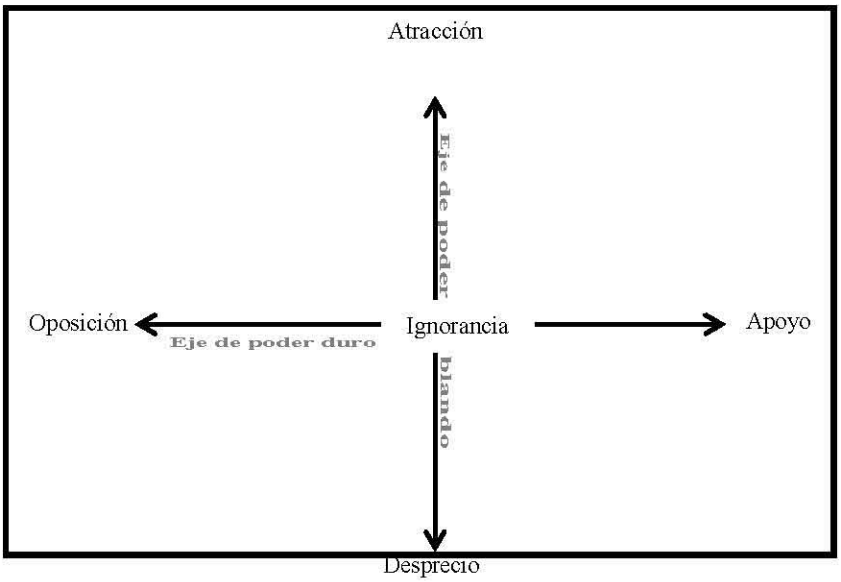
Elaboración propia con información de John Arquilla en *Redes y guerras en red: el futuro del terrorismo, el crimen organizado y el activismo político*. Madrid: Alianza, 2003., pp. 184-194.

En cuanto al bloqueo a los medios de interconexión, es difícil pensar que esta condición pueda mantenerse por mucho tiempo como se ha observado a lo largo de la historia, la tendencia de un país a aislarse de las demás naciones no es muy aconsejable. Un punto substancial en este sentido es la cuestión económica, puesto que constituye un pilar esencial para todo Estado es imposible imaginar que la interacción global de los mercados no logre permear la esfera social.

[155] Cáceres Sebastián. "El acceso a Internet en los países subdesarrollados". *Observatorio de la Sociedad de la Información*, Fundación auna. [En línea] Disponible en: <http://fundacionorange.es/areas/28_observatorio/pdfs/subdesarrollados.pdf>. (Consulta 28/08/2013).

En otro orden de ideas, los Estados deben aprender a interactuar con movimientos sociales. Puesto que Internet ha logrado colocarlos en la escena internacional hoy día su presencia es cada vez más importante; sería aconsejable establecer foros de interacción en donde organizaciones civiles, gobiernos y público en general puedan intercambiar opiniones sobre determinados asuntos. Respecto a las autoridades y su interacción con los nuevos movimientos sociales, según Luther P. Gerlach, profesor de antropología de la Universidad de Minnesota, las posibles soluciones se orientan en dos sentidos: 1) el poder blando, mediante acciones sutiles como el dialogo o influyendo en la opinión pública, sin tomar medidas militares; 2) el poder duro, oponiéndose abiertamente a estos grupos, tomando medidas de contención o disuasión, o formando alianzas en su contra. Aunque por lo general la estrategia emprendida, de acuerdo con Gerlach, es una combinación de ambos poderes[156] (véase figura 4).

Figura 4. Directivas de acción para tratar con los actores no estatales organizados en la red



Fuente: Arquilla, John. *Redes y guerras en red: el futuro del terrorismo, el crimen organizado y el activismo político*. Madrid: Alianza. 2003., p. 370

Sin lugar a dudas, la capacidad de expresión y comunicación global que otorgan las nuevas tecnologías le han dado cierto optimismo a los movimientos sociales particularmente con respecto a la democracia. Pierre Lévy (2004) profesor de la Universidad de Ottawa,

[156] Ronfeldt y Arquilla. *Óp. Cit.*, pp. 368-370.

platea que las TIC brindan mayor libertad, y que se están desarrollando de forma sorprendente nuevas capacidades de organización y socialización. En términos generales, planea Lévy, la llegada de la Era informática ha traído consigo una corriente democratizadora caracterizada por mayores conexiones y nuevas oportunidades de cooperación, democracia, emancipación, justicia y transparencia. Respecto a esta transformación vale la pena analizar dos casos importantes: las movilizaciones en Túnez, y las recientes manifestaciones en Turquía. En ambos el rol de las nuevas tecnologías ha sido determinante.

Túnez representa el primer caso de organización y movilización social desde la red, surgió a raíz de la manifestación de Mohamed Bouazizi frente al ayuntamiento de Sidi Bouzid.[157] Bouazizi protestó en contra de un régimen autoritario y el despotismo de sus autoridades; el joven tunecino se prendió fuego en plena calle; tiempo después sería conocido como el mártir que dio el primer paso hacia la liberación nacional. El papel de las tecnologías en este caso es muy importante, pues la generación que creció y se desarrolló a la par de las TIC encontró en la web un espacio libre para organizarse y manifestarse políticamente. Las redes sociales demostraron su capacidad organizativa y lo reflejaron en las manifestaciones que dieron lugar a la caída de Zine Abidine Ben Ali. Las agrupaciones en línea y la comunicación electrónica permitieron que todo el mundo fuera testigo de lo estaba ocurriendo en tiempo real. Indudablemente surgieron intentos de bloquear los medios electrónicos, las autoridades emplearon a 2 000 trabajadores de la Agencia Tunecina de Internet (ATI), dando inicio a una batalla cibernética en contra de los disidentes del régimen, quienes a su vez fueron apoyados por el grupo hacker *Anonymous*.[158] Al tiempo en que gobierno tunecino intentaba controlar el flujo de información en la red, activistas y expertos en TIC creaban nuevos atajos para comunicarse, pues el intercambio de mensajes fue crucial para la organización de manifestaciones. Hace unas décadas difícilmente hubiese sido posible observar —en tiempo real— movilizaciones sociales de otras partes del mundo, hoy gracias a las innovaciones tecnológicas se ha derrumbado la barrera distancia-tiempo.

---

[157] Parreño, Antonio. (Enero 3, 2012). "El chico que se quemó e incendió el mundo árabe". *Rtve*. [En línea]. Disponible en: <http://www.rtve.es/noticias/20120103/mohamed-bouazizi-chico-no-pudomas/482545.shtml>. (Consulta 29/05/2013).

[158] Isabelle Mandraud. (Enero 17, 2011). "En Tunisie, la révolution est en ligne ". *Le Monde*. [En línea]. Disponible en:<http://www.lemonde.fr/afrique/article/2011/01/17/en-tunisie-la-revolution-est-en-ligne_1466624_3212.html>. (Consulta 20/06/2013).

Lo más importante es que fue posible conocer la opinión de quienes formaban parte del movimiento y gracias a los mensajes vertidos en *Twitter* y *Facebook* la población mundial una versión alterna al de las autoridades oficiales. Otro punto importante es que los connacionales que se encontraban en otras partes del globo podían apoyar la causa a través *World Wide Web* para dar proyección mundial al conflicto. Por medio de sitios electrónicos, agencias de noticias y organizaciones civiles se ponían al alcance de todos videos, audios, fotografías, testimonios, reportajes, etc. que mantenían a la sociedad global constantemente informada. Al mismo tiempo, el mundo entero esperaba la respuesta de actores internacionales como la Organización de Naciones Unidas o la Unión Europea mientras que Amnistía Internacional daba a conocer la cantidad de víctimas resultado de las frecuentes represiones. La indignación de Mohamed Bouazizi ante la corrupción y nepotismo de Ben Ali se contagió al resto del país y entre algunas naciones del mundo árabe. Aunque antes del 17 de noviembre —fecha en que Bouazizi protestó— gran parte del mundo desconocía lo que ocurría en Túnez, sólo unos días después la comunidad internacional rechazaba abiertamente la represión a las manifestaciones sociales y se pronunciaba a favor de la libre expresión y de la democracia. En *Twitter*, *Facebook* y demás foros en red la juventud tunecina compartía con el mundo su inconformidad por la falta de oportunidades y la permanencia de sistema despótico.

Por parte de los actores en la red, el grupo *Anonymous* atacó los sitios web estatales y la bolsa de valores; en las redes sociales, la cuenta *Nawaat de Tunisie*—encargada de publicar el rumbo de las movilizaciones y el número de manifestantes detenidos— contaba con 17 000 seguidores al 6 de enero de 2011, de acuerdo con diario *Clarín*.[159] Ya en febrero de 2009 *WikiLeaks* había dado a conocer un reporte elaborado por el *United States Congressional Research Service* (centro de investigaciones estadounidense) en el que además de denunciar la corrupción del régimen y demostrar el dominio del parlamento por parte del *Constitutional Democratic Rally* (partido del Ben Ali), se evidenciaba la violación

[159]Herrera de Noble, Ernestina. (Enero 6, 2011). "Rebelión popular y masivo ataque de hackers en Túnez". *Clarín*. [En línea]. Disponible en: <http://www.clarin.com/mundo/Rebelion-popular-masivo-hackers-Tunez_0_404359596.html>. (Consulta 21/05/2013).

de derechos humanos en Túnez.[160] Algunos especialistas como Isabelle Mandraud, colaboradora de *Le Monde*, han propuesto llamarla "La revolución Facebook", pues la rapidez rapidez y sencillez para propagar mensajes en las redes sociales colaboró, en gran medida, a la la movilización social. Al respecto las autoridades esperaban, inútilmente, que al detener a unos unos cuantos ciberactivistas recuperarían la pasividad en la calles, por el contrario cada detención suscitó nuevas marchas. Rápidamente surgieron foros, grupos y cuentas en la red, alentando a la población a levantarse en contra de un régimen con más de 20 años en el poder. La comunidad internacional apoyó la transición hacia un sistema democrático. Sin embargo, aunque la red de redes hizo posible un cambio de régimen los objetivos de libertad, democracia, igualdad y justicia que inspiraron el movimiento todavía hoy están muy lejos de alcanzarse.

El siguiente caso posee mayor complejidad, pues debido a que el conflicto en Turquía surgió hace muy poco tiempo y al día de hoy se encuentra en constante movimiento, analizarlo resulta un tanto complicado; sin embargo es preciso examinarlo, pues no se trata de una protesta de la Primavera árabe, ni tampoco en busca de una transición democrática, fue más bien la incapacidad de las autoridades para comprender una manifestación social que sólo buscaba proteger un área ecológica.

Todo empezó cuando el gobierno decidió convertir el parque *Taksim Gezi* (en Estambul) en un centro comercial. En respuesta, el 28 mayo de 2013, la población salió a las calles para manifestarse en contra de dicha medida. Dos días después las protestas exigían la renuncia del Primer Ministro Recep Tayyip Erdogan,[161] a partir de entonces la represión se convirtió en el principal mecanismo para enfrentar las protestas. Las declaraciones oficiales señalaban a las redes sociales como principal culpable, y la constante represión que dejó como resultado cientos de presos y algunos heridos, sirvieron como catalizador para que, poco a poco, cientos de personas se sumaran a las manifestaciones que terminaron extendiéndose en otras partes del territorio. De nuevo las TIC colocan en el centro del debate la capacidad de las autoridades para aceptar una sociedad informada y participativa. Lejos de condenar a las redes sociales deben

[160] Reporte RS21666. (Febrero 2, 2009). *WikiLeaks*. [En línea]. Disponible en: <http://wlstorage.net/file/crs/RS2666.pdf>. (Consulta 16/01/2013).

[161] "Turquía vive tercera jornada de violentas protestas". (Junio 3, 2013) *El Universal*. [En línea] Disponible en: <http://www.eluniversal.com.mx/notas/927100.html>. (Consulta 28/04/2013).

comprender que se trata de un nuevo espacio público en donde el gobierno puede interactuar con la opinión de la mayoría. De una simple protesta a favor del medio ambiente las manifestaciones en Turquía se convirtieron en una demanda para transformación del pues, después de que el Primer Ministro Erdogan hiciera una declaración en contra del uso las redes cibernéticas en los movimientos sociales aumentó la cantidad de personas reunidas en las calles, el Primer Ministro declaró: "hay una maldición llamada *Twitter*. Son puras mentiras [...] Eso a lo que llaman redes sociales son la maldición de la sociedad hoy en día".[162] No es suficiente detener a unos cuantos "alborotadores" en *Twitter* y *Facebook* cuando lo que está en juego es la libertad de expresión y la participación política de la ciudadanía.

¿Qué hubiera pasado si en lugar de enfrentar las protestas con violencia las autoridades se hubieran abierto al dialogo; si en lugar de rechazar el uso de Internet lo adoptaran como una vía de comunicación con la sociedad? Hasta el momento la comunidad internacional reconoce que el gobierno turco fue incapaz de responder adecuadamente a la opinión manifiesta de la ciudadanía, en este caso no se trata de una transición de régimen, sino de transformarse (o evolucionar) en un gobierno más abierto, transparente y con la participación de la mayoría en el proceso de toma de decisiones. La situación de Turquía se encuentra en un periodo difícil y sin duda representa un reto para la capacidad de control de los Estados; abrirse a las nuevas tecnologías obstruyendo la participación política no es una buena combinación; en este caso sería posible reinterpretar el lema turco: "libertad y participación política en las redes, paz en casa y en el mundo".

La llegada de una nueva era dominada por las TIC plantea diferentes retos a las autoridades nacionales e internacionales. La Sociedad de la información surgió gracias al desarrollo de diversas tecnologías, en especial Internet, que han hecho posible un intercambio universal de conocimiento. Este nuevo panorama permite que día a día sea posible interactuar socialmente con distintas partes del mundo, por lo que cada individuo se convierte en una especie de *ciberciudadano*. La globalización y el desarrollo tecnológico transformaron simultáneamente la realidad, hoy día la innovación tecnológica permite que

[162] "Twitter, una maldición para la sociedad, acusa Turquía". (Junio 3, 2012) *El Universal*. [En línea]. Disponible en: <http://www.eluniversal.com.mx/notas/927283.html>. (Consulta 13/05/2013).

los ciudadanos sean conscientes de distintos contextos sociales y acontecimientos mundiales, siendo capaces de percibir la forma en que repercuten en su propio entorno, en adición su respectivo poder de acción también se ha modificado. Los movimientos sociales manifiestan la opinión de la ciudadanía, pueden reunir a miles de personas entorno a un mismo propósito; la llegada de la Era tecnológica no sólo ha transformado las comunicaciones, también al principal elemento en ellas: el hombre. La llamada "Sociedad del conocimiento" demanda una nueva forma de interacción con el Estado, un reto nada fácil y que sin duda ha quedado demostrado con el comportamiento de las autoridades en los casos antes mencionados.

Para la sociedad contemporánea resulta imposible cohabitar con autoridades del siglo pasado. La necesidad de comprender las nuevas formas de expresión y manifestación es imperante para todos los representantes estatales; los casos de bloqueo de comunicaciones y represión social siempre reflejan la incapacidad de quienes están en el poder. Es preciso que la aceptación de la sociedad red no sólo se quede en el discurso deben implementarse nuevos canales de comunicación con la ciudadanía no sólo para la estabilidad de una nación, también para su pleno desarrollo.

De acuerdo Pierre Levy (2004), sólo aquellas sociedades que sean capaces de abandonar el viejo modelo donde la mayoría está en la base y sólo unos cuantos en la cima serán capaces de funcionar eficazmente. Aunque los alcances de las nuevas tecnologías e Internet aún son limitados se han dado importantes avances en la propagación de las TIC, que sin duda transforman el panorama social, económico y político en todo el mundo; en la actualidad 2.7 mil millones de personas, casi el 40% de la población mundial, tienen acceso a la red de redes,[163] ¿cómo responderán las autoridades a esto? Para finalizar resulta conveniente rescatar la afirmación de Tiffany Danits

> *La ventaja de la red es que es diplomática. Promueve el dialogo entre quienes están en sociedades cerradas y el mundo exterior* […] *cada parte puede utilizar el foro que ofrece Internet, para explicar sus propuestas dentro de un*

[163] ITU. *The World in 2013 - ICT Facts and Figures.* [En línea]. Disponible en: <http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2013.pdf>. (Consulta 02/06/2013).

contexto global [...] *quizá no llegue a ser un auténtico debate, pero es el comienzo.*[164]

3.9. Consecuencias políticas para Internet

La red se ha convertido progresivamente en el principal medio de enlace de millones de personas alrededor del mundo. Sin embargo, al tiempo en que representa un invaluable avance tecnológico también constituye un riesgo para las naciones. La cantidad y tipo de información que circula por la *Word Wide Web* cada día es impresionante; el ciberespacio necesita normas que procuren la adecuada convivencia entre sus participantes, pero ¿cómo controlar un espacio intangible y sin límites estatales? La dificultad no sólo recae en encontrar mecanismos adecuados para la regulación de Internet, también en aquellos organismos que se encargarán de aplicarlos, pues debe establecerse un punto equilibrado para no caer ni en autoritarismo, ni en anarquía. Sin embargo, antes de analizar las consecuencias políticas para ciberespacio producidas por *WikiLeaks* es importante examinar, en forma general, cuales son los desafíos que representa el uso de las TIC para la seguridad del sistema internacional. En este aspecto a pesar del aumento en el número de participantes dentro la dinámica mundial el Estado-nación continúa siendo el actor principal, y también el único encargado de proporcionar mecanismos eficientes de seguridad para sus ciudadanos y de cooperar bajo este mismo objetivo con otras naciones. En el ámbito social las nuevas tecnologías se han convertido en un elemento esencial para las comunicaciones, pero también han incrementado la importancia del concepto de seguridad en muchos sectores. En la actualidad el alcance de las TIC puede ser visto como un beneficio o como una amenaza para el bienestar de la sociedad. Las dimensiones de este nuevo desafío todavía son desconocidas, aunque ya se han observado algunos alcances, es indudable que también puede afectar de distintas formas el funcionamiento de una nación debido a la creciente dependencia de las actividades diplomáticas, políticas, económicas y militares, hacia las nuevas herramientas tecnológicas. De esta forma, por ejemplo, las dimensiones en las que un ataque informático puede dañar a un Estado son incalculables. Al respecto George Tenet ex director de la Agencia Central de Inteligencia de EE.UU. (CIA por sus siglas en inglés)

[164] En Arquilla, John. (2003). *Redes y guerras en red: el futuro del terrorismo, el crimen organizado y el activismo político*. Madrid: Alianza p. 182.

sugiere que en la Era tecnológica, un ataque digital puede ser tan peligroso como un ataque con misiles intercontinentales en la Era nuclear. [165]

El fenómeno *WikiLeaks* demostró la urgencia de mecanismos eficientes capaces de salvaguardar la confidencialidad de las comunicaciones oficiales, las consecuencias de la publicación de cables clasificados son en parte previsibles, entre ellas está el establecimiento de medidas más rígidas entorno al control de flujo de información que circula entre naciones y en el propio territorio. Aunado ello surge la necesidad de cooperación internacional en la materia, pues como apunta Lorenzo Valeri (2007) establecer límites en la jurisdicción de un Estado se torna complicado cuando se traslada el escenario al ciberespacio.[166] Lo más probable es que se refuercen los mecanismos de cooperación en materia legal para la persecución y castigo de delitos informáticos, así como las disposiciones para el intercambio de datos en entre naciones, de la misma forma las medidas que se establezcan en el plano nacional se orientaran en el control del intercambio de datos entre ciudadanos. Entre las consecuencias inmediatas se puede prever el endurecimiento de las sanciones a los delitos relacionados con espionaje y sustracción ilícita de documentos clasificados, y el impulso de instrumentos jurídicos internacionales en la materia.

No obstante, a pesar de los intentos por regular el ciberespacio la web seguirá siendo el más importante reto jurídico para la sociedad contemporánea. Al respecto Carles Alonso (2011),profesor de Derecho Constitucional, afirma que de no encontrar soluciones adecuadas en el terreno práctico, la respuesta consistirá en mejorar las nociones de objetividad, transparencia y participación, dentro de los Estados, pues más que prohibir portales web dedicados a las filtraciones, lo que se debe procurar son mejores mecanismos de rendición de cuentas a la ciudadanía, y en el caso de la diplomacia contemporánea adoptar medidas socialmente más incluyentes y transparentes.

Internet se ha convertido en una herramienta clave para la escena mundial a tal grado que ha logrado modificarla. En este mismo sentido Myriam A. Dunn, profesora en estudios de seguridad estratégica, señala que los cambios cuantitativos—provocados por la revolución

---

[165] Eriksson, Johan y Giampiero Giacomello. (2007). *International Relations and Security in the Digital Age.* Reino Unido: Routledge.

[166] Valeri, Lorenzo. (2007). *Public- private cooperation and information assurance: a liberal institutionalism approach*. En Eriksson, Johan. *Óp. Cit.* pp., 132-157.

informática— en los modelos, patrones, prácticas e instituciones han logrado transformar también cualitativamente el sistema internacional.[167] Es posible concluir que el entorno modifica el comportamiento del sujeto, por lo tanto si las características y condiciones del escenario internacional se han transformado, la interacción internacional entre los Estados también lo ha hecho, por ello es necesario que las normas que regulan las relaciones internacionales y a los propios sujetos también lo hagan; quizá la velocidad del cambio ha impedido establecer medidas adecuadas que respondan a la nueva realidad, aunado a esto dicha transformación no es un proceso terminado sino uno constante movimiento, lo que implica el surgimiento de interacciones internacionales más dinámicas e interdisciplinarias, por lo que representa un importante desafío.

El fenómeno *WikiLeaks* plantea un gran reto para el aparato jurídico moderno, pues deben establecerse normas que aseguren la privacidad en los asuntos del Estado, sin perjudicar nociones como la libertad de expresión de los medios de comunicación y el derecho a la información de los ciudadanos.

[167] Dunn, Myriam A. (2007).*Securing the digital age: the challenges of complexity for critical infrastructure protection and IR theory*. En: Eriksson Johan, *Óp. Cit.*, pp. 85-105.

Capítulo 4. El caso *WikiLeaks* en Canadá

Los documentos publicados por *WikiLeaks* en 2010 impactaron de forma directa no sólo a Estados Unidos, sino también a todas aquellas naciones con las que mantenía relaciones diplomáticas, entre ellas Canadá. Las continuas transformaciones políticas y sociales, así como la complejidad y transcendencia de este país en el orbe internacional obligan a analizar los efectos que el fenómeno generó en la política, los medios de comunicación y la sociedad canadiense.

Todo comenzó en julio de 2010, cuando el portal web *WikiLeaks* publicó 92 000 bitácoras de EE.UU. sobre la guerra en Afganistán; poco después los servicios de inteligencia y de seguridad de la administración Obama sufrirían otro golpe, ya que en octubre de ese mismo año el portal difundió 392 000 reportes pertenecientes al Pentágono relacionados con el conflicto en Iraq. No obstante, las repercusiones generadas por dichas revelaciones son menores a las que ocasionó la divulgación de 251 187 cables diplomáticos del gobierno estadounidense que también involucraban a múltiples Estados. La forma en que Estados Unidos se relacionaba con otros países fue evidenciada a nivel mundial, pues las filtraciones dieron a conocer el alcance de su participación en otras naciones, los temas abordados en reuniones oficiales y hasta observaciones personales elaboradas por representantes de Washington.[168] Entre tanto la prensa internacional se dedicó a analizar los temas más controversiales, ya que las filtraciones se relacionaban con cuestiones como seguridad nacional, tratados comerciales, conflictos bélicos, negociaciones internacionales, terrorismo, etc. Como consecuencia el principal afectado no sólo fue el gobierno estadounidense, sino también aquellas naciones con las que mantenía vínculos.

En el caso de Canadá las filtraciones llevaron al alcance de todos comunicaciones confidenciales relacionadas con: regulaciones medioambientales, el clima político interno, la percepción canadiense sobre Estados Unidos, los derechos indígenas, la intervención de Washington en temas de seguridad e inteligencia, la participación canadiense en Afganistán, entre muchos otros. Estos tópicos colocaron en el centro del escenario la imagen que Canadá

[168] Sánchez Hernández, Carlos. (Marzo, 2011). "Analogías de la Historia I: Julian Assange y WikiLeaks vs Daniel Ellsberg y los Pentagon Papers". *Nómadas. Revista Crítica de Ciencias Sociales y Jurídicas*, no. 31. [En línea]. Disponible en: <http://pendientedemigracion.ucm.es/info/nomadas/31/carlosschzhernandez.pdf>. (Consulta 11/11/2013).

proyecta al exterior, y el poder de influencia que Estados Unidos tiene en la nación. Ante esta situación vale la pena analizar cuáles fueron las revelaciones más importantes, su contenido, el impacto que generaron —tanto en la opinión pública como en la élite política canadiense— y sus principales repercusiones.

4.1. Revelaciones más importantes

Canadá se caracteriza en el plano internacional como una nación con alto grado de consciencia ecológica; un país que posee poder "moral" en el escenario mundial, y cuya diversidad geográfica, y cultural, reflejan la gran capacidad de tolerancia y negociación aplicada tanto a nivel interno como externo. Sin embargo, Canadá (como cualquier otro país) posee tópicos capaces de confrontar múltiples opiniones, en el ámbito político las dificultades para llegar a un consenso, las divergencias ideológicas, la complicada interacción entre las provincias y el gobierno federal, entre otros temas, denotan la existencia de una sociedad diversa y participativa. En este contexto las revelaciones de *WikiLeaks* impulsaron o reanimaron cuestiones complejas para la política nacional e internacional canadiense.

El 26 de noviembre de 2010 Washington advirtió a Canadá —y a otros Estados como Reino Unido, Australia, Israel, Noruega y Dinamarca— sobre las revelaciones que *WikiLeaks* publicaría días después.[169] Ante esta situación, el entonces Ministro de Relaciones Exteriores, Lawrence Cannon, declaró a los medios de comunicación que las filtraciones no perjudicarían la relación con Estados Unidos.[170] Posteriormente se divulgaron 2 421 notas diplomáticas pertenecientes a embajadas y consulados, causando diversas reacciones en los planos político y social,[171] pues los cables evidenciaron el nivel de autoridad que Estados Unidos posee en temas como seguridad (donde, incluso, ha llegado a participar en temas de interés nacional). En este sentido las declaraciones de Cannon

---

[169] EFE. (Noviembre 26, 2010). "EE.UU. alerta a 6 Gobiernos por la próxima filtración de Wikileaks". *Lavanguardia.com*. [En línea]. Disponible en: <http://www.lavanguardia.com/20101126/54075422576/ee-uu-alerta-a-6-gobiernos-por-la-proxima-filtracion-de-wikileaks.html>. (Consulta 11/11/2013).

[170] Marcano, Edgar (Noviembre 29, 2010). "Fugas de Wikileaks: Lawrence Cannon no está preocupado". *Despertar Dominicano*. [En línea]. Disponible en: <http://www.despertardominicano.com/noticias/noticias-de-canada/197-fugas-de-wikileaks-lawrence-cannon-no-esta-preocupado>. (Consulta 21/11/2013).

[171] Nelson, Marissa. (Noviembre 28, 2010). "WikiLeaks reveals undiplomatic U.S. critiques". *CBC News*. [En línea]. Disponible en: <http://www.cbc.ca/news/world/wikileaks-reveals-undiplomatic-u-s-critiques-1.878000>. (Consulta 26/11/2013).

provocaron que la prensa canadiense se cuestionara si las excesivas intervenciones habían ocurrido con el consentimiento de las autoridades.[172]

Entre las publicaciones que generaron mayor polémica están las relacionadas con: 1) medio ambiente; 2) seguridad nacional; 3) los derechos indígenas; 4) la percepción estadounidense en Canadá; 5) normas multilaterales, y 6) la presencia canadiense en Afganistán.

1) Respecto al medio ambiente los cables denotaron las divergencias existentes entre el entonces Primer Ministro quebequense Jean Charest y Stephen Harper respecto a la postura federal en la reunión de Copenhague sobre cambio climático; ya que anteriormente durante una visita (a Quebec) del embajador norteamericano David Jacobson, Charest compartió su interés por que Canadá logre comprometerse a reducir la emisión de gases de efecto invernadero, postura de la que Harper difiere radicalmente, al considerar que con ello se perjudicaría la economía nacional.[173]

2) Con relación a la seguridad nacional las filtraciones revelaron las actividades de inteligencia estadounidense en Canadá. En una filtración relacionada con el caso "Toronto 18" (escrita en febrero 2010)[174] se puede observar que las autoridades canadienses compartieron información confidencial a Washington relacionada con investigaciones judiciales; el mismo cable informa al gobierno estadounidense que los mandos canadienses no habían detenido todavía a todos los involucrados, y se ponía en duda la efectividad del RCMP.[175]

3) Otro tema sensible y que sin duda afecta la percepción nacional e internacional del gobierno en turno son los derechos indígenas. En este sentido los documentos también reflejan

---

[172] Marcano, Edgar. *Óp. Cit.*

[173] Descôteaux, Bernard. "NDLR: Extraits des portions du câble diplomatique qui touchent la conférence de Copenhague, la position du Québec et l'influence de la famille Desmarais". *Le Devoir.* [En línea]. Disponible en: <http://www.ledevoir.com/wikileaks-power>.(Consulta 23/11/2013).

[174] "Toronto 18" se refiere a una operación que realizaron autoridades canadienses en dicha ciudad en 2006, cuando 400 policías fuertemente armados ingresaron a los hogares y detuvieron a una gran cantidad de jóvenes argumentando que se buscaba impedir un ataque terrorista. El caso fue hábilmente manejado por las autoridades en los medios de comunicación, en donde afirmaron que jóvenes musulmanes radicales se estaban organizando en mezquitas canadienses y por medio de Internet para ejecutar el más grande ataque terrorista en la historia canadiense. Fuente: Miller, John y Cybele Sack (*s.f.*)

[175] La Real Policía Montada de Canadá, RCM, por sus siglas en inglés *Royal Canadian Mounted Police.*

la "débil" definición de las autoridades con relación a los derechos de las minorías.[176] En esta cuestión *WikiLeaks* reactivo la polémica, pues las revelaciones impulsaron un interesante debate a través de múltiples blogs sobre el tema, un ejemplo es *Warrior Publications* de la plataforma *Wordpress*, donde se analizan filtraciones relacionadas con la participación del FBI (Oficina Federal de Investigación de EE.UU.) en el conflicto entre autoridades canadienses e indígenas en Kanesatake (Quebec) en 2004.[177]

4) Un punto interesante es abordado en el cable 08OTTAWA136 donde se analiza la percepción nacional sobre Estados Unidos. Al respecto, los representantes de Washington reportaron una tendencia antiestadounidense en los medios de comunicación que —de a sus observaciones— reflejan desconfianza hacia gobierno de Barack Obama.[178]

5) Uno de los asuntos que mayor debate han generado en la sociedad es la construcción de normas multilaterales. Donde, de acuerdo a las publicaciones, Estados Unidos ejerce presión para que Canadá adopte regulaciones sobre propiedad intelectual compatibles con el Acta de cese a la piratería en línea, SOPA, (por siglas en inglés) para lo cual utiliza el Acuerdo Estratégico Transpacífico de Asociación Económica; en concreto busca la extensión de los derechos de autor por 20 años más (hoy en día la vigencia máxima es de 50 años),[179]lo cual repercutiría en sectores tan sensibles como el farmacéutico. Adicionalmente plantea una regulación para los proveedores de Internet con disposiciones como eliminar derechos de acceso de los suscriptores, el bloqueo de contenido e, incluso, el monitoreo de actividades en línea.[180]

---

[176] Borthwick, Meg. (Mayo 4, 2011). "WikiLeaks comes to Canada: Federal failure on aboriginal rights". *Rabble.ca*. [En línea]. Disponible en: <http://rabble.ca/news/2011/05/wikileaks-comes-canada-federal-failure-aboriginalri>. (Consulta 20/11/2013).

[177] Hill, Gord. (Mayo 4, 2011). "Wikileak Warriors: US cables on Native 'threats'". *Warrior Publications*. [En línea]. Disponible en: <http://warriorpublications.wordpress.com/2011/05/04/wikileak-warriors-us-cables-onnativeta>. (Consulta 21/12/2013).

[178] WikiLeaks. (Enero 25, 2008). "Primetime Images of US-Canada Border Paint U.S. In Increasingly Negative Light". *Cablegatesearch.net*. [En línea]. Disponible en: <http://www.cablegatesearch.net/cable.php?id=08OTTAWA136&q=08ottawa136>. (Consulta 21/12/2013).

[179] WikiLeaks. (Noviembre 13, 2013). "Secret TPP treaty: Advanced Intellectual Property chapter for all 12 nations with negotiating positions". [En línea]. Disponible en: <http://wikileaks.org/tpp/static/pdf/Wikileaks-secret-TPPtreaty-IP-chapter.pdf>. (Consulta 10/12/2013).

[180] Geist, Michael. (Noviembre 19, 2013). "Leaked TPP Text Confirms Countries Had Plenty to Hide". *Michael Geist's Blog*. [En línea]. Disponible en: <http://www.michaelgeist.ca/content/view/7001/135/>. (Consulta 21/01/2014).

6) Otra cuestión transcendente es la participación canadiense en Afganistán, en este sentido *WikiLeaks* señala que durante 2009 el gobierno canadiense enfrentó presiones de Estados Unidos para extender su participación en Oriente Medio. En los documentos los representantes de Ottawa señalaron que lo más difícil sería impacto de esta decisión en la opinión pública, por lo que solicitaron paciencia por parte del gobierno de Obama. La nota diplomática (09OTTAWA218) menciona que para Stephen Harper, Afganistán representaba un tema políticamente sensible del que la facción liberal buscaba obtener ventaja. En ese entonces el líder de la oposición Michael Ignatieff señaló que Harper faltaría a su palabra extendiendo la misión canadiense en Kandahar (Afganistán). A pesar de todo la solicitud de Washington fue concedida; no obstante, el Primer Ministro Harper se apresuró a señalar que si la misión permanecería sería sólo en calidad de no combatiente.[181]

Es oportuno mencionar que a pesar de la enorme cantidad de documentos los que consiguieron mayor atención fueron los relacionados con la protección ambiental, dado que es un tema en el que diversos políticos concentran sus esfuerzos para mantener la imagen internacional canadiense de "país responsable y comprometido". Sin embargo, las divergencias del grupo conservador en este punto han enfrentado a múltiples actores, puesto que frecuentemente temas como la seguridad energética y la economía nacional se contraponen a la responsabilidad canadiense con el medioambiente.

Respecto a las relaciones con Estados Unidos, es posible observar el rechazo a la injerencia estadounidense en cuestiones de seguridad, así como en el establecimiento de normas de propiedad intelectual. Este último punto ha causado inconformidad en la esfera social, ya que se percibe como un desafío a la soberanía nacional. Como consecuencia la independencia de las instituciones nacionales ha sido cuestionada, ya que los cables sugieren una cooperación excesivamente estrecha con Estados Unidos. Los alcances de esta participación se reflejan en reportes de inteligencia relacionados con seguridad nacional que se compartieron con la administración Obama sin una justificación razonable.

[181] Hildebrandt, Amber. (Mayo 13, 2011). "Canada reconsidered Afghan combat end date: WikiLeaks". *CBC* News. En línea]. Disponible en: <http://www.cbc.ca/news/canada/canada-reconsidered-afghan-combat-end-date-wikileaks-1.988520>. (Consulta 21/12/2013).

En cuanto a las consecuencias inmediatas, Tom Flanagan, ex jefe de gabinete del Primer Ministro Stephen Harper, comentó ante *CBC News* que Julian Assange (editor en jefe de *WikiLeaks*) debería ser asesinado, también le sugirió al presidente Obama contratar a o utilizar un avión no tripulado para dicho objetivo. Las declaraciones de Flanagan causaron controversia, pues la cadena para la que trabaja como comentarista recibió varias quejas por declaraciones,[182]aunque días después Flanagan se retractó, sus comentarios llegaron hasta el Parlamento donde John Baird, representante de la Cámara de los Comunes, señaló que los comentarios de Flanagan no reflejaban la opinión de Canadá, ni la del Primer Ministro. Por su parte el delegado liberal Denis Coderre presentó una denuncia contra *CBC News* por "incitar a la violencia".[183] En cuanto a los medios canadienses se puede observar una gran variedad de opiniones, de entre las que destaca la escritora y columnista Ezra Levant, quien considera al trabajo de *WikiLeaks* como espionaje y no como periodismo.[184]

Mientras tanto los simpatizantes de *WikiLeaks* han creado un portal web dedicado a las filtraciones canadienses, en la plataforma se pueden consultar las revelaciones por provincia, ciudad e importancia además de ser un foro de discusión también se ocupa de analizar temas actuales;[185] otra página electrónica es *cablegatesearch.net* una especie de filtro que permite encontrar publicaciones con base en diferentes criterios, y el cual presenta unos 10 330 enlaces referentes a Canadá.[186]

4.2. Los efectos en el escenario político

Es difícil calcular el grado en que *WikiLeaks* afectó la práctica política en Canadá (tanto a nivel nacional como a nivel internacional), ya que se trata de un fenómeno cuyo alcance y contenido resulta inconmensurable. Sin embargo, existen casos que permiten analizar los efectos que la publicación de información oficial generó en la esfera política canadiense.

---

[182] The Canadian Press. (Diciembre 3, 2010). "WikiLeaks founder calls for Flanagan charge". *CBC News*. [En línea]. Disponible en: <http://www.cbc.ca/news/politics/wikileaks-founder-calls-for-flanagan-charge-1.877546>. (Consulta 26/12/2013).

[183] The Associated Press. (Diciembre 1, 2010). "Flanagan regrets WikiLeaks assassination remark". *CBC News*. [En línea]. Disponible en: <http://www.cbc.ca/news/politics/flanagan-regrets-wikileaks-assassination-remark1.877>. (Consulta 11/12/2013).

[184] *Ídem.*

[185] Canada wiki. (Septiembre 25, 2013). *Reddit*. [En línea]. Disponible en: <http://www.reddit.com/r/canada/wiki/relatedsubreddits>. (Consulta 20/12/2013).

[186] WikiLeaks. *WikiLeaks Canada*.Cablegateseach. [En línea]. Disponible en: <http://www.cablegatesearch.net/search.php?q=canada&sort=1>. (Consulta 27/12/2013).

Al respecto uno de los factores a favor de *WikiLeaks* es que permitió confirmar la autenticidad de las publicaciones a través del acceso a la documentación oficial, lo que innegablemente repercutirá en la conformación de la opinión pública, y por ende, en la legitimación de las decisiones políticas. Por lo tanto es evidente que las publicaciones cambiarán el rumbo de las negociaciones en torno a ciertas iniciativas de ley, y modificarán la la forma en la que los actores políticos manejan determinados asuntos.

Un efecto inmediato fue que la regulación de Internet se convirtió en tema central dentro del Parlamento canadiense, generando toda una discusión en torno a las ventajas y desventajas del uso de las TIC en la sociedad y en las estructuras gubernamentales. Es por ello que a continuación se examinará el impacto que *WikiLeaks* generó tanto en el ámbito político nacional como en el internacional canadiense.

4.2.1. A nivel nacional

En el plano nacional las repercusiones de *WikiLeaks* se orientan en dos direcciones; la primera se relaciona con las filtraciones que involucraron directamente a personalidades políticas canadienses, y la segunda con las reacciones generadas en el aparato legislativo con el fin de prevenir nuevas filtraciones, controlar el flujo de información en Internet y estructurar medidas eficaces de ciberseguridad.

Respecto al primer punto, el contenido de las filtraciones logró comprometer a varios políticos canadienses y a sus partidos. En este sentido, el cable 10OTTAWA29 describe cómo el partido conservador busca beneficiarse políticamente incluyendo en su discurso la preocupación por el norte; para el gobierno estadounidense es claro que Stephen Harper no tiene ningún interés por el Ártico, ya que no ha implementado las medidas adecuadas para aumentar la vigilancia en el paso del noroeste. De acuerdo con el cable es evidente que el partido conservador ha hecho del Ártico una marca política en su búsqueda por conseguir electores. El documento escrito por David Jacobson (Embajador estadounidense en Canadá desde 2009) establece que Stephen Harper ha utilizado la preocupación por el Ártico para beneficiarse durante las campañas de 2006 y 2008. La filtración refleja que el discurso utilizado por el entonces candidato a Primer Ministro difiere mucho de su opinión personal, ya que en múltiples ocasiones ha tenido oportunidad de discutir esta cuestión con diversos representantes

estadounidenses y, sin embargo, en ninguna tocó el tema.[187] Ante estas publicaciones Andrew McDougall, entonces vocero de Harper, declaró que las filtraciones sólo hacían referencia a algunos compromisos y que Canadá es un país consiente de sus obligaciones, también afirmó que el gobierno en turno siempre ha respaldado sus declaraciones con acciones.[188]

Como estas cuestiones existen otras más que involucran varios aspectos del gobierno canadiense, las más controversiales sin duda se relacionan con la protección al medio ambiente, pero también incluyen asuntos bilaterales como la discusión en torno a *Devil's Lake*. Como su nombre lo indica se trata de un lago ubicado en Dakota del norte y que ha logrado confrontar a los gobiernos de Dakota y Manitoba. Los cables diplomáticos señalan que la actitud del entonces Primer Ministro de Manitoba Gary Doer imposibilitó que ambos gobiernos pudieran llegar a una solución; la problemática consiste en que a lo largo de 70 años el nivel del lago ha aumentado 16 metros, amenazando numerosas granjas de Dakota del Norte. En búsqueda de una solución el gobierno estadounidense se pronuncia a favor de desviar la desembocadura del lago, mientras que Canadá teme por el equilibrio ambiental. Tras la publicación el autor de la nota (David Wilkins) lamentó el alcance de sus observaciones —pues consideró que el lamentable estado de las negociaciones reflejaba el fracaso diplomático de Canadá— y aseguró Gary Doer es reconocido como un excelente diplomático en Estados Unidos.[189] Sin embargo, a pesar de las declaraciones la negociación entorno a *Devil's Lake* sigue sin avanzar.

Finalmente una de las publicaciones más debatidas es la relacionada con Jean Charest y su relación con *Power Corp.* Jean Charest fue Primer Ministro de Quebec de 2003 a 2012, y siempre se ha mostrado en contra de la posición federal en materia de cambio climático. Sin embargo, tras la revelación del cable 10MONTREAL1_a, la opinión pública respecto a

---

[187] Jacobson, David. (Enero 21, 2010). *10OTTAWA29, Canada's Conservative Government and its Arctic Focus*. WikiLeaks. [En línea]. Disponible en: <http://wikileaks.org/cable/2010/01/10OTTAWA29.html>. (Consulta 14/01/2014).

[188] The Canadian Press. (Mayo 12, 2011). "WikiLeaks: U.S. dismisses Harper's Arctic talk". *CBC News*. [En línea]. Disponible en: <http://www.cbc.ca/news/canada/wikileaks-u-s-dismisses-harper-s-arctic-talk-1.1009886>. (Consulta 13/01/2014).

[189] Nelson, Marissa. (Junio 6, 2011). "WikiLeaks shows bitter Canada-U.S.". *CBC News*. [En línea]. Disponible en: <http://www.cbc.ca/news/canada/manitoba/wikileaks-shows-bitter-canada-u-s-water-tiff-1.1073888>. (Consulta 13/12/2014).

Charest cambió, pues la filtración revela una posible influencia de Paul Desmarais (director general de *Power Corporation*) sobre el ex Primer Ministro. En este sentido los diarios canadienses se han dedicado a analizar el repentino cambio de posición en Charest. En el documento, escrito por David Jacobson se critica la participación del Charest durante la conferencia de Copenhague, lo que dio paso a una guerra de declaraciones entre el diario *La Presse* y *Le Journal* (de Montreal) respecto a los vínculos financieros del ex Primer Ministro con el director de *Power Corporation* (cabe aclarar que *La Presse* es propiedad de *Gesca* que a que a su vez es subsidiaria de *Power Corp*).

Luego del encuentro en Copenhague *La Presse* salió en defensa del gobierno federal y de su opinión con relación a las arenas bituminosas, lo que sorprendió a la prensa quebequense, pues rara vez el periódico está a favor de Ottawa. Mientras tanto en Quebec la posición de Charest fue reconocida; en contraste en Ottawa *La Presse* le calificó de desleal. Por su parte el ex embajador Jacobson señaló que si Charest optó por una posición débil en Copenhaguese debió a la influencia de la familia Desmarais y de *La Presse*.[190] Ante todo esto Charest se negó a hacer una declaración oficial, limitándose a señalar que siempre ha trabajado por los intereses de Quebec.[191]

La cuestión de las arenas bituminosas confronta a múltiples sectores en Canadá, por un lado existe todo un poder corporativo que ha logrado influir en la estructuración de políticas orientadas al medio ambiente, y que no sólo se ha limitado al ámbito político, sino también a los medios de comunicación donde existen diversas publicaciones que defienden la explotación de las arenas de Alberta sin importar el costo ambiental. Por otro lado están aquellas provincias preocupadas por el medio ambiente, y que se esfuerzan por el desarrollo de fuentes alternativas de energía como Quebec, Ontario, Columbia Británica, Nueva Escocia, entre otras;[192] también existen actores políticos preocupados por impulsar una mejor legislación para la conservación y

[190] Radio-Canada. (Mayo 11, 2011). "Charest se défend d'être influencé par Power Corp.". *CBC News*. [En línea]. Disponible en: <http://www.radio-canada.ca/nouvelles/Politique/2011/05/11/003-charest-powercorpwikilaks.>. (Consulta 14/01/2014).

[191] Nelson, Marissa. (Mayo 11, 2011). "Photo Galleries Charest defends against WikiLeaks report". *CBC News*. [En línea]. Disponible en: <http://www.cbc.ca/news/canada/montreal/charest-defends-against-wikileaks-report-1.1058273>. (Consulta 14/01/2014).

[192] Holburn, Chico LF *et. al.* (Junio, 2013). "La energía eólica en Canadá: Un Estudio del Medio Ambiente Política." *Ivey Energy Policy and Management Centre*. [En línea]. Disponible en: <http://sites.ivey.ca/energy/files/2013/07/3554-Ivey-Energy-Wind-Policy-v04.pdf>. (Consulta 13/01/2014).

protección del medio ambiente. Sin embargo, cada postura suele confrontarse, por un lado, con el costo económico que conllevaría abandonar la explotación de las arenas bituminosas, y por el otro, con el impacto ambiental que a la larga repercutirá en el sector más importante: la población.

Pasando al siguiente punto —las reacciones generadas en el aparato legislativo— el tema *WikiLeaks* ha sido analizado desde distintas perspectivas por el Parlamento canadiense a de diversos comités especializados. El primero de ellos fue la onceava reunión del Comité Especial Antiterrorismo, donde se analizó el impacto que la divulgación de una lista de infraestructura crítica en Canadá podría generar en la seguridad nacional. En la sesión se examinó el uso de Internet por parte de organizaciones terroristas para obtener información valiosa en la estructuración de ataques; también se discutieron las repercusiones que la publicación de cables sobre Medio Oriente puede generar en el ejercicio diplomático canadiense. El grupo de expertos señaló que las revelaciones de *WikiLeaks* afectaron la cooperación en materia de inteligencia, establecida con otros gobiernos; por ello se determinó mejorar los mecanismos de protección de datos.[193]

Desde otra perspectiva, Scott Brison miembro del parlamento por Kings—Hants percibe al fenómeno *WikiLeaks* como un desafío a los mecanismos de resguardo de datos financieros. Con la divulgación de 2 000 cuentas bancarias transfronterizas pertenecientes al *Julius Baer Bank & Trust Company Ltd.*,[194] *WikiLeaks* representa un reto internacional, impulsado por la globalización y la evolución tecnológica, para optimizar los instrumentos de monitoreo y protección de datos financieros. Por esta razón diversos funcionarios canadienses han propuesto la creación de un extranet multilateral, aunque para Brison establecer un instrumento de esta naturaleza sólo aumentaría la vulnerabilidad de los datos

[193] ONCEAVA REUNIÓN DEL COMITÉ ESPECIAL DEL SENADO EN ANTI-TERRORISMO (11: 2010: Ottawa). Tercera sesión del cuadragésimo Parlamento de Canadá. Ottawa: Diciembre 6, 2010. [En línea]. Disponible en: <http://www.parl.gc.ca/Content/SEN/Committee/403/anti/48515e.htm?comm_id=597&Language=F&Parl=40&Ses=3>. (Consultada 15/01/2014).

[194] Finch, Gavin y Warren Giles. (Enero17, 2011). "WikiLeaks to Publish Data from Ex-Julius Baer Banker". *Bloomberg L.P.* [En línea]. Disponible en: <http://www.bloomberg.com/news/2011-01-17/wikileaks-to-publish-client-datafrom-ex-julius-baer-banker.html>. (Consulta 11/01/2014).

financieros, dado que al encontrarse reunidos en una sola plataforma los alcances de una filtración serían mayores.[195]

Por otra parte, en 2012 el Comité Permanente del Senado sobre Seguridad y Defensa Nacional examinó el contenido de las filtraciones respecto a la guerra en Afganistán. Para Jack Jack Granatstein (investigador distinguido del Instituto canadiense de Defensa y Asuntos Exteriores) a pesar de que publicar material confidencial es un acto delictivo, los cables ofrecieron información importante sobre la verdadera historia del conflicto en Medio Oriente.[196] En la reunión —que tenía como objetivo valorar las lecciones de Canadá en la guerra guerra en Afganistán— se admitió que los datos disponibles respecto a esta clase de asuntos son limitados, y que es necesario informar a la ciudadanía lo más apegados a la realidad cuando se tocan dichos temas.

Para finalizar, el fenómeno *WikiLeaks* ha confirmado lo que Manuel Castells (2009) llama "política informacional". De acuerdo con Castells la evolución tecnológica ha generado cambios en la política y en los procesos democráticos, que se reflejan en la trasformación del debate político y de las estrategias para obtener el poder. En este sentido gran parte del impacto de las filtraciones se debe a la enorme difusión otorgada por los medios de comunicación, que de acuerdo con Castells se han convertido en un elemento esencial para ejercer influencia política. Desde esta perspectiva los medios de información han incrementado su influjo sobre la opinión pública, lo que a su vez, modifica el comportamiento de los actores políticos, transformando la relación entre el Estado y la sociedad. Ante dicho escenario las revelaciones de *WikiLeaks* indudablemente generarán cambios en la estructuración y aplicación de estrategias políticas. Castells también declara que el surgimiento de filtraciones convierte a los medios de comunicación en un campo de batalla en la lucha por el poder, y ello confirma el incremento del peso de la opinión pública. Otro efecto de *WikiLeaks* en el ámbito político es la reconsideración de la privacidad y de la protección de los datos que circulan en el ciberespacio (tanto en el ámbito financiero, como en el político y social). Interpretando a Castells es posible

[195] 59ª REUNIÓN DEL COMITÉ PERMANENTE DE FINANZAS (59: 2011: Ottawa). Tercera sesión del cuadragésimo Parlamento de Canadá. Ottawa: Febrero 17, 2011. [En línea]. Disponible en: <http://www.parl.gc.ca/HousePublications/Publication.aspx?DocId=4977520&Language=E&Mode=1>.(Consulta 10/01/2014).

[196] QUINTA REUNIÓN DEL COMITÉ PERMANENTE DEL SENADO SOBRE SEGURIDAD NACIONAL Y DEFENSA (5: 2012: Ottawa). Tercera sesión del cuadragésimo Parlamento de Canadá. Ottawa: Marzo 26, 2012. [En línea]. Disponible en: <http://www.parl.gc.ca/content/sen/committee/411%5CSECD/05EVA-49438-e.HTM>. (Consulta 14/03/2014).

afirmar que lo importante en las revelaciones de *WikiLeaks* no son los datos que informa sino el debate que genera alrededor, pues eso constituye su más valiosa aportación.

4.2.2. A nivel internacional

En cuanto a las repercusiones en el ámbito internacional existen diversas valoraciones de *WikiLeaks*; por una parte están quienes sostienen que las relaciones de Canadá con el resto del mundo no se verán afectadas, y por el otro lado, quienes consideran que las filtraciones cambiarán radicalmente la profesión diplomática.

Sin embargo, existen cuestiones en donde la tensión es mayor, como en las operaciones contra el terrorismo por parte de Estados Unidos y Canadá, también surgen cuestiones como las negociaciones multilaterales en torno al establecimiento de normas para los derechos de autor y la regulación de Internet. En este sentido la filtración de las medidas que en el marco del Acuerdo de Asociación Transpacífico, TPP (por sus siglas en inglés), Estados Unidos se esfuerza por imponer —orientadas a la regulación de Internet— y que afectarían la privacidad de los ciudadanos[197] constituye un punto crítico, pues al igual que los documentos relacionados con los derechos de autor han generado una gran discusión, en este aspecto se busca el establecimiento de normas muy estrictas y completamente alejadas de la regulaciones internacionales.[198]

Las negociaciones del TPP se caracterizaban por su secretismo, por lo que las resoluciones alcanzadas difícilmente podían ser conocidas por el público en general, sin embargo, con las publicaciones de *WikiLeaks* la sociedad ha podido construir una idea sobre el contenido de los convenios. El Acuerdo de Asociación Transpacífico también dificultaría la ejecución de normas nacionales, pues enfrentaría las disposiciones del Acuerdo con las medidas planteadas por el gobierno canadiense a través de la iniciativa C-8 relacionada con el combate a la falsificación.[199] Por dicha situación es difícil pensar que el establecimiento

---

[197] Geist, Michael. (Noviembre 18, 2013). *The TPP IP Chapter Leaks: U.S. Wants New Regulations for Country-Code Domain Names.* [Blog]. Disponible en: <http://www.michaelgeist.ca/content/view/7002/125/>. (Consulta 21/01/2014).

[198] Geist, Michael. (Noviembre 19, 2013). *Leaked TPP Text Confirms Countries Had Plenty to hide.* [Blog]. Disponible en: <http://www.michaelgeist.ca/content/view/7001/135/>. (Consulta 21/01/2014).

[199] Geist, Michael. (Noviembre 15, 2013). *The TPP IP Chapter Leaks: U.S. Demanding Overhaul of Canadian Anti-Counterfeiting Bill.* [Blog]. Disponible en: <http://www.michaelgeist.ca/content/view/6997/125/>. (Consulta 21/01/2014).

de normas multilaterales en el marco del TPP será sencillo, ya que la presión estadounidense a Canadá ha generado inconformidad en gran parte de la población, que hoy día demanda mayor participación en la estructuración de la política exterior.

Por otra parte, la publicación de una red de espionaje operando en Irán (que constantemente constantemente monitorea las actividades de Hezbolá) afectará las relaciones de Canadá con Medio Oriente. *WikiLeaks* también reveló observaciones que Jim Judd, entonces director del Servicio de Inteligencia Canadiense, CSIS (por sus siglas en inglés), elaboró sobre Hamid Karzai (Presidente de Afganistán). Judd expresó que Harzai mantenía una posición débil en un gobierno lleno de corrupción, con problemas de tráfico de drogas y con un poder limitado en las fuerzas judiciales. El ex director de inteligencia también expresó la desconfianza del gobierno canadiense por tratar con "armas de doble filo" como Irán (con quien estableció comunicación entorno a Afganistán). Asimismo las revelaciones incluyeron acuerdos de una minera canadiense en Kirguistán en medio de un imperante clima de corrupción, aunque el cable no revela el nombre de la minera la fecha del encuentro permite deducir que se trata de *Kumtor Gold Company*.[200]

Un tema que también es interesante es la participación canadiense en la invasión Iraq, donde los cables reflejan una posición un tanto contradictoria por parte de las autoridades, pues mientras ante el público en general mantenían una posición en contra de la guerra, dentro de las comunicaciones confidenciales con Washington proponían que el ejército canadiense se movilizara en Iraq; también se reveló que Canadá había participado en el plan de invasión a Bagdad, incluso, meses antes de la declaratoria oficial, y aunque la presencia canadiense en el Estrecho de Ormuz era oficialmente parte del apoyo a la liberación, el cable señala que prestaron manera extraoficial otros servicios.[201]

Como ésta existen otras publicaciones que reflejan la verdadera naturaleza de la política exterior canadiense. Sin embargo, por un lado la complejidad de este tipo de cuestiones demanda confidencialidad de cualquiera de las partes, pues como se ha observado la posición

[200] Freeze, Colin. (Agosto 23, 2012). "Canadian spy secrets exposed in WikiLeaks dump".*The Globe and Mail.* [En línea]. Disponible en: <http://m.theglobeandmail.com/news/politics/canadian-spy-secrets-exposed-in-wikileaks-dump/article1316198/?>.(Consulta 21/01/2014).

[201] Bronski, Carl. (Mayo 19, 2011). "Wikileaks cable exposes Canadian duplicity in Iraq war". *World Socialist Web Site*. [En línea]. Disponible en: <https://www.wsws.org/en/articles/2011/05/cana-m19.html>. (Consulta 24/01/2014).

respecto a determinas conflictos, y las operaciones de inteligencia en áreas peligrosas, entre otros aspectos, podrían vulnerar la seguridad de los Estados involucrados. Por otro lado la publicación de negociaciones entorno el establecimiento de normatividad multilateral a la ciudadanía, pues coloca a su alcance información relevante, que afecta directamente a la sociedad, y denotan la necesidad de reportes públicos sobre ésta clase de disposiciones.

En resumen, la aplicación de nuevas tecnologías en el ámbito internacional posee ventajas y desventajas, el impacto de *WikiLeaks* en la política internacional canadiense hace un llamado a la aplicación de estándares éticos y legales para tratar este nuevo desafío, y confirma que tanto individuos como gobiernos se enfrentan a un ecosistema desconocido que requiere de nuevas estrategias, normas y principios para funcionar adecuadamente.[202]

De acuerdo con Castells (2001) la "política de los escándalos" es un arma predilecta para luchar y competir en la política internacional, puesto que los nuevos medios han reafirmado su poder en el escenario mundial; en este sentido las acciones a favor de un gobierno transparente pueden deslegitimizar a los actores políticos y, en última instancia, a la democracia activa.

4.3. El impacto en la sociedad

El arribo de la era tecnológica ha transformado los mecanismos de interacción entre la sociedad y el Estado. La web como herramienta de comunicación e información también ha modificado la naturaleza de la participación ciudadana, prueba de esto son diversas manifestaciones masivas que han recorrido el mundo durante los últimos años, y donde las TIC facilitaron la coordinación, comunicación y difusión de distintos movimientos. Por ello tanto la ciudadanía como las naciones son conscientes de lo implica la llamada "democratización de la información".

Dado que la proyección de la acción colectiva ha aumentado con uso de nuevos dispositivos electrónicos y en especial de Internet, hay quienes consideran que la red de redes es la contribución más importante para la paz en el mundo. Sin embargo, la web posee límites como cualquier otra vía de comunicación, y no es inmune a ser controlada; un ejemplo de esto son las

[202] Deibert, Ron. (Diciembre 11, 2010). "The Post-Cablegate Era". *The New York Times*. [En línea]. Disponible en: <http://www.nytimes.com/roomfordebate/2010/12/09/what-has-wikileaks-started/after-wikileaks-a-new-era>. (Consulta 23/01/2014).

prácticas de monitoreo a organizaciones activistas a través de Internet, que demuestran las desventajas de encontrarse en un mundo interconectado.

WikiLeaks reanimó el debate canadiense en torno a la participación ciudadana en el proceso de toma de decisiones; del mismo modo se retomaron cuestiones como los derechos de las minorías, la estructuración de normas para la regulación de Internet, el establecimiento de leyes sobre derechos de autor, entre otros temas. Con ello la sociedad encontró la posibilidad de ampliar el foro de discusión, adoptando formas de expresión como el hacktivismo, y especialmente con el surgimiento de movimientos organizados en Internet como *Occupy Canada*.

Una consecuencia evidente de la actividad de *WikiLeaks* en Canadá es la creación de un portal quebequense dedicado a la publicación de filtraciones con el objetivo de establecer un gobierno transparente: QuebecLeaks, que también está vinculada con la organización hacktivista *Anonymous*[203] y ha declarado simpatizar con el proyecto de Julian Assange (*WikiLeaks*).[204]

De forma general la ciudadanía desea que su voz sea escuchada tanto en el proceso de estructuración de normas, como en la toma de decisiones del gobierno canadiense. Por lo tanto la participación social a través de la web se orienta hacia la búsqueda de un gobierno abierto, donde la innovación tecnológica sirva de enlace entre la sociedad y el Estado.

4.3.1. Movimientos sociales

A través del tiempo la sociedad canadiense ha experimentado diversos cambios —especialmente después de la Segunda Guerra Mundial[205]— que colaboraron a la construcción de la ciudadanía contemporánea. Históricamente las movilizaciones sociales han enarbolado

[203] Grou, Vincent. (Febrero 8, 2011). "WikiLeaks inspire QuébecLeaks". *Sur le Web*. [En línea]. Disponible en: <http://blogues.radio-canada.ca/surleweb/2011/02/08/wikileaks-inspire-quebecleaks/>. (Consulta 27/12/2013).
[204] QuebécLeaks. (2013). *What is QuebécLeaks?* [En línea]. Disponible en: <https://www.quebecleaks.org/en/about-us/what-is-quebecleaks/>. (Consulta 28/12/2013).
[205] Tras la Segunda Guerra Mundial Canadá aceptó a 165 000 refugiados procedentes de Gran Bretaña, Italia, Alemania, Holanda y Hungría. A finales del siglo XX la sociedad canadiense estaba compuesta por inmigrantes provenientes de diversas naciones entre ellas Bosnia, Ruanda, Kosovo y Vietnam. Para 2005 más de la mitad del índice de crecimiento poblacional estaba conformado por migrantes. Fuente: Political Culture Researchomatic (Diciembre, 2011). *Social Movements in Canada*. [En línea]. Disponible en: <http://www.researchomatic.com/Political-Culture-98036.html>. (Consulta 23/12/2013).

diversas demandas como: a favor de los derechos de los migrantes y de los grupos indígenas; en busca de mejores servicios de seguridad social; en pro del medio ambiente, etc. Con el paso de los años las nuevas formas de participación ciudadana y la colaboración entre diversos grupos activistas han marcado diferentes etapas en la evolución de la sociedad en Canadá.

Durante la segunda mitad del siglo XX, en especial durante el periodo del Primer Ministro John Diefenbaker (1957 – 1963), Canadá enfrentó una fuerte crisis económica que generó altos índices de desempleo, como consecuencia Diefenbaker fue removido de su cargo en abril de 1963 para ser remplazado por el liberal Lester Pearson. A partir de entonces, y con el apoyo del partido Nueva Democracia, Pearson implementó una serie de medidas con el fin de establecer mejores condiciones de vida. Como resultado dio inicio un periodo donde la sociedad participó activamente en la vida política nacional, muestra de ello es la creación del *Royal Commission of the Status of Women* en febrero de 1967, la institución tenía como objetivo analizar las medidas que el gobierno debía adoptar para garantizar la igualdad entre hombres y mujeres. Otro paso importante fue el establecimiento de la red de seguridad social de 1968, que otorgó servicios de salud gratuitos a toda la población. Por otra parte desde 1920 diversas organizaciones de trabajadores han luchado por conseguir mejores condiciones laborales como lo son jornadas y salarios más justos, y mayores prestaciones.

Bajo esta misma línea desde 1930 surgieron importantes grupos a favor de los derechos humanos y de las libertades civiles que experimentaron su momento cumbre durante el periodo de 1960 a 1980. De acuerdo con Dominique Clement (2008) los años sesenta representaron la época de esplendor de activismo canadiense; grupos en defensa de los derechos de los homosexuales, organizaciones a favor del aborto, agrupaciones en busca de la equidad de género, entre otros, emergieron en la escena social. A lo largo de más de 20 años la ciudadanía manifestó libremente su opinión respecto a distintos temas, solicitando que su voz fuera escuchada por quienes estructuraban las normas que dirigían la nación. El ejercicio activista que marcó la época se materializó en organismos como *The National Action Committee on the Status of Women* (de 1972), *The Urban Alliance on Race Relations* —a favor de los derechos de los Afroamericanos— (de 1975), *The Gay Alliance towards Equality* (de 1971), y en entidades en defensa de las libertades civiles como *British Columbia Civil Libertés Association* (de

1962), *Ligue des droits de l'homme* —a favor de los derechos humanos, y del ciudadano—(de 1898), entre otras. [206]

Como es posible observar, la sociedad canadiense ha transitado por diversas etapas en los últimos años, dichas transformaciones fueron impulsadas por eventos como el surgimiento de nuevas tecnologías, el fenómeno de la globalización y las trasformaciones políticas de finales de siglo.

Al respecto un episodio importante en la historia de los movimientos sociales (a nivel general) son los acontecimientos de Seattle en 1999. Las protestas con motivo del Encuentro Ministerial de la Organización Mundial del Comercio denotaron la existencia de una generación impaciente, deseosa de formar parte de las resoluciones políticas de su propia nación y de impulsar una transformación mundial. Durante cinco días cerca de 50 000 personas se manifestaron en Seattle para denunciar el establecimiento de medidas neoliberales que buscaban incrementar los beneficios del comercio internacional sin tomar en cuenta el bienestar humano ni el medioambiente.[207] Las manifestaciones de 1999 son importantes porque consiguieron la atención de la prensa internacional a través de medidas tan drásticas como el bloqueo al recinto donde se llevaría a cabo la sesión inaugural y de calles aledañas; 41 autobuses procedentes de Ontario, Manitoba, Vancouver, Saskatchewan, Alberta y Columbia Británica[208] llegaron al estadio de Seattle para sumarse a la causa.[209] Diversas organizaciones sociales (entre ecologistas, agrupaciones a favor de los derechos humanos, sindicatos, etc.) se reunieron bajo un sólo objetivo. El 30 de noviembre de 1999 será recordado porque miles de jóvenes de distintas partes del mundo se unieron en torno a una demanda: "otro mundo es posible".[210] A través de la gran cantidad de información disponible en línea sobre la lucha en Seattle, Internet mostró los primeros indicios de su potencial a favor de las movilizaciones

[206] Clemente, Dominique. (2008). *Canada's Rights Revolution*. Canadá: UCB Press.
[207] Harter, John-Henry. (2011). *New Social Movements, Class, and the Environment: A Case Study of Greenpeace Canada*. Cambridge Scholars Publishing. [En línea]. Disponible en: <http://www.c-s-p.org/flyers/978-1-4438-2863-5-sample.pdf>. (Consulta 23/12/2013).
[208] DTP. "Countdown to the Battle of Seattle". *Do or Die*, no. 9, pp. 129-133. [En línea]. Disponible en: <http://www.eco-action.org/dod/no9/seattle_chronology.html>. (Consulta 23/12/2013).
[209] Jaff, Dave. (Enero, 2000). "Unitarians join Seattle protest against the WTO". *The Canadian Unitarian*, vol. 41, no. 1, pp. 1-2. [En línea]. Disponible en: <http://cuc.ca/wp-content/uploads/2011/10/January2000.pdf>. (Consulta 23/12/2013).
[210] Antentas, Josep María y Esther Vivas. (Diciembre, 2009). "De Seattle a la crisis global Viento del sur". *Viento Sur*, no. 107, pp. 30-40. [En línea]. Disponible en: <http://www.vientosur.info/articulosabiertos/VS107_AtentasyVivas_ DeSeattlealacrisis.pdf>. (Consulta 23/12/2013).

sociales. Sin embargo, la sociedad internacional todavía no conocía la extensión de sus alcances.

Poco después en las protestas de Toronto (en 2010) en contra de la reunión del G-20 dieron como resultado casi 600 detenidos— las redes sociales reafirmaron su utilidad en la lucha social.[211]Posteriormente a finales de ese mismo año las manifestaciones de la árabe, el surgimiento de los movimientos *Occupy together* y las movilizaciones estadounidenses contra las reformas a las normas de seguridad médica y de migración demostraron que la "Sociedad del conocimiento" no permanecería inactiva por mucho

La influencia de *WikiLeaks* en el activismo canadiense se proyecta en el surgimiento del movimiento *Occupy Wall Street*, impulsado por la activista Heather Marsh en el portal *WL Central*. Marsh apoyaba la idea de un movimiento que transformara a Canadá y al resto del mundo,[212] poco después *WikiLeaks* emprendió una campaña para dar a conocer el proyecto.[213] Un apoyo importante para *Occupy* fue el trabajo de la revista canadiense sin fines de lucro *Adbusters* quien colaboró a la denominación del movimiento,[214] y cuyo principal objetivo es denunciar la influencia de las corporaciones en la democracia, la distribución inequitativa de la riqueza en el mundo y el manejo irresponsable de la economía global que ha producido incesantes crisis económicas. Progresivamente el ideal de las protestas se contagió a otras partes del mundo.

En Canadá el movimiento *Occupy together* se propagó en Alberta, Columbia Británica, Manitoba, Nuevo Brunswick, Terranova y Labrador, Ontario, Nueva Escocia, entre otras provincias, tomando como pieza fundamental la comunicación vía redes sociales. Bajo la demanda "descolonizar el sistema", el movimiento *Occupy Canada* busca reparar el

---

[211] AVN. (Junio 27, 2010). "Policía detiene a casi 600 manifestantes durante Cumbre del G-20". *Sibci*. [En línea]. Disponible en: <http://static1.avn.info.ve/contenido/polic%C3%ADa-detiene-casi-600-manifestantes-durante-cumbre-del-g-20>. (Consulta 23/12/2013).

[212] Si bien Heather Marsh buscaba una transformación global, la idea del movimiento *Occupy Wall Street* fue estructurada, primordialmente, por la activista neoyorkina Alexa O'Brien (que en un principio lo nombró *US Day of Rage*).

[213] Dorling, Philip. (Octubre 29, 2011). "Assange can still Occupy centre stage". *The Sidney Morning Herald*. [En línea]. Disponible en: <http://www.smh.com.au/technology/technology-news/assange-can-still-occupy-centre-stag e-20111028-1mo8x.html>. (Consulta 21/11/2013).

[214] Flemingh, Andrew. (Septiembre 27, 2011). "Adbusters sparks Wall Street protest". *Vancouver Courier*. [En línea]. Disponible en: <http://www.vancourier.com/news/adbusters-sparks-wall-street-protest-1.374299>. (Consulta 21/11/2013).

deteriorado contrato social y reivindicar la democracia. *Occupy* también adoptó demandas de grupos indígenas, al respecto *Occupy Winnipeg* ha incorporado el respeto a la soberanía indígena como parte fundamental de sus peticiones.[215]

Uno de los grandes logros del movimiento fueron las protestas en contra de las reducciones reducciones a la vivienda y a los servicios públicos impulsadas por el alcalde de Toronto, Rob Rob Ford; el 12 de enero de 2012 cerca de 3 000 personas se manifestaron frente al *City Hall Hall* (construcción que alberga el ayuntamiento de Toronto) para rechazar estos ajustes. Finalmente las protestas lograron vencer la iniciativa de un recorte presupuestal de aproximadamente 20 millones de dólares.[216]

En síntesis, pese a que la sociedad canadiense se caracteriza por ser políticamente participativa las revelaciones de *WikiLeaks*, junto a la ola de protestas que se suscitaron a la postre, le han otorgado un nuevo impulso. Prueba de ello es el impacto generado en la opinión pública en una encuesta elaborada por *Abacus Data* (Octubre, 2011) de 1 005 canadienses encuestados, el 41% tenía una impresión favorable del movimiento *Occupy Canada*. Lo más importante del efecto *WikiLeaks* es que distintos grupos sociales presentaron una perspectiva diferente sobre problemática nacional. En adición, la comunidad canadiense desea: mantenerse informada de las cuestiones más importantes de la política nacional a través de diversas iniciativas; formar parte de la estructuración de normas, y —lo mejor de todo— mantener vivos debates como los derechos de las minorías y la protección al medio ambiente. Quizá el efecto inmediato de las filtraciones no fue del todo trascendente, pero las repercusiones a largo plazo en la ciudadanía serán más grandes, movilizaciones como *Occupy Together* le demostraron al mundo que la "Sociedad de la información" es más que sólo un concepto y que de ahora en adelante proyectará su opinión a través de nuevos medios. No significa que Internet sea el instrumento más grande para cambiar el mundo, pero genera debate, es capaz de reunir miles de opiniones respecto a un sólo tema, confronta perspectivas y propuestas de cambio de cientos de individuos alrededor del mundo, incentiva el dialogo nacional e internacional, y es precisamente ahí donde se puede generar una transformación.

---

[215] Kilibarda, Konstantin. (2012). "Lessons from #Occupy in Canada: Contesting Space, Settler Consciousness and Erasures within the 99%". *Journal of Critical Globalisation Studies*, no. 5, pp. 24-41. [Enlínea]. Disponible en: <http://www.criticalglobalisation.com/issue5/24_41_OCCUPY_IN_CANADA_JCGS5.pdf>. (Consulta 26/12/2013).
[216] *Ídem.*

4.3.2. El hacktivismo canadiense

El hacktivismo es el uso no violento de herramientas tecnológicas legales, o ilegales, con de difundir un mensaje político.[217] En otras palabras se trata de una nueva modalidad de para que los grupos activistas puedan manifestarse. Hay quienes consideran que el hacktivismo —al igual que otras formas de expresión— debe recibir algún tipo de protección legal, pero existen múltiples obstáculos cuando se desea definir qué actividades cibernéticas deben estar permitidas, y cuáles no. Al respecto los métodos más utilizados de hacktivismo son: deshabilitar sitios web, sustraer información, realizar críticas irónicas o burlescas en portales electrónicos, ataques DoS,[218] y sabotajes. Por lo tanto existen formas de ciberexpresión que pueden generar graves daños económicos en las víctimas.

Sin embargo, el derecho a la libre expresión no debe ser un elemento excluido del ciberespacio. Existen diversos casos en donde el hacktivismo ha colaborado a la difusión de demandas sociales especialmente en países donde la libertad de expresión se encuentra excesivamente restringida. No obstante, el carácter anónimo y los alcances internacionales de esta nueva forma de protesta han llevado a considerarla uno de los grandes desafíos del siglo XXI para los Estados-nación.

Por otra parte, es un hecho que la sociedad contemporánea ha incorporado a la vida cotidiana el uso de herramientas tecnológicas, y al igual que diversas naciones, ONG y organismos internacionales utilizan la web (y las redes sociales) para intercambiar datos y comunicarse con el mundo, desde esta perspectiva el hacktivismo aparece como una forma legítima de protesta, ya que es capaz de dar proyección a las voces que normalmente son silenciadas, difunde crímenes en contra de la humanidad y violaciones a las libertades civiles o a los derechos humanos. Sin embargo, debe ser ejercido con responsabilidad, pues

---

[217] Hampson, Noah C.N. (Enero 5, 2012). "Hacktivism: A New Breed of Protest in a Networked World". *Boston College International and Comparative Law Review* (artículo 6), vol. 35, no. 2. [En línea]. Disponible en: <http://lawdigitalcommons.bc.edu/cgi/viewcontent.cgi?article=1685&context=iclr>. (Consulta 26/12/2013).

[218] Ataques de Denegación de Servicio, DoS, (por sus siglas en inglés) están diseñados para dificultar, o paralizar completamente, el funcionamiento de un sitio web, red, servidor electrónico u otro recurso. Generalmente, consiste en sobrecargar los servidores con incesantes solicitudes de acceso hasta que las plataformas se vuelven tan lentas que los usuarios son incapaces de acceder al portal web o los servidores terminan colapsándose. Fuente: Kaspersky Lab (1996-2014). "Ataque DoS". *Viruslist.com*. [En línea]. Disponible en: <http://www.viruslist.com/sp/glossary?glossid=153602817>. (Consulta 26/12/2013).

al igual que en el mundo real existe una gran diferencia entre una protesta pacífica y un motín.[219]

La historia del hacktivismo canadiense inicia en julio de 1998, cuando se llevó a cabo una importante reunión entre dos famosos activistas electrónicos en Toronto —Blondie Wong (director de *Hong Kong Blondes*)[220] y Oxblood Ruffin (Ministro de Relaciones Exteriores de *The Cult of the Dead Cow*)[221]— , en donde discutieron las formas con las que la comunidad hacker podía colaborar en la lucha a favor de los derechos humanos, y actuar en contra de políticas comerciales poco éticas. El encuentro tenía como objetivo presionar a las corporaciones americanas, evidenciando su comportamiento en China.[222]

Poco después en febrero del 2000 una serie de ataques DDoS[223] inhabilitaron los portales web de compañías como *Amazon*, *CNN*, *Dell*, *eBay* y *Yahoo*. El culpable: un hacker de sólo 17 años, que fue condenado a ocho meses de custodia abierta.[224] El caso atrajo la atención de medios nacionales e internacionales, al punto en que autoridades estadounidenses participaron en la investigación. La defensa de "Mafiaboy"[225] alegó que las actividades habían sido ejecutadas en beneficio de la comunidad, ya que se habían identificado las debilidades de los sistemas atacados, y de esta forma se había impulsado la optimización de los mecanismos de

---

[219] Hampson. *Óp. Cit.*

[220] *Hong Kong Blondes* es uno de los primeros grupos hacktivistas en China, está conformada por expertos en el ámbito de la computación y activistas en pro de los derechos humanos y la democracia. Fuente: Trinity-hackers (2013). "The Hong Kong Blondes". *Creative Commons Attribution Share-Alike.* [En línea]. Disponible en: <http://trinity-hackers.wikispaces.com/The+Hong+Kong+Blondes>. (Consulta 27/12/2013).

[221] *The Cult of the Dead Cow* es una de las más conocidas agrupaciones hacktivistas y quien, se siguiere, creó el concepto de hacktivismo.

[222] Ruffin, Oxblood. (Julio 15, 1998). "The Longer March: Interview with Blondie Wong". *cDc communications #356*. [En línea]. Disponible en: <http://www.cultdeadcow.com/cDc_files/cDc-0356.html>. (Consulta 28/12/2013).

[223] Denegación de Servicio Distribuida o DDoS por sus siglas en inglés (*Distributed Denial of Service*). Es una ampliación de los ataques DoS (véase nota 211). Consiste en la instalación de varios agentes remotos en múltiples computadoras que pueden estar ubicadas en diversas partes del mundo. El invasor es capaz de coordinar todos los agentes para lanzar un ataque masivo. Fuente: Prolexic (2003-2014). "What is DDoS denial of service?" *Knowledge Center*. [En línea]. Disponible en: <http://www.prolexic.com/knowledge-center-what-is-ddos-denial-ofservice.htl>. (Consulta 27/12/2013).

[224] *Open custody*: orden de la Corte que consiste en una especie de condena seccionada, donde el menor debe cumplir dos terceras partes de la misma en un centro especializado, y la tercera parte bajo supervisión de la comunidad. Fuente: Newfoundland and Labrador (Enero 10, 2014). "Open Custody". *Departament of Child, Youth and Family Services.* [En línea]. Disponible en: <http://www.gov.nl.ca/cyfs/youthcorrections/opencustody.html>. (Consulta 27/12/2013).

[225] Seudónimo asignado por los medios, dado que la ley canadiense prohíbe revelar públicamente la identidad de un menor.

defensa. La noticia provocó que el concepto de "hacktivismo" fuera intensamente analizado, tanto en los medios de comunicación como en la sociedad y en la esfera política Entre tanto las autoridades estadounidenses declararon que Canadá se estaba convirtiendo en una especie de paraíso para los hackers.[227]

A la postre el término "ciberterrorismo" emergió en múltiples discursos políticos, lo que provocó, de acuerdo con Gary Genosko (2006) que la situación se sintetizara a la siguiente ecuación: hacking + activismo + ciberespacio = ciberterrorismo. Como consecuencia en la prensa canadiense declaró que Internet podría ser un arma para las organizaciones de esta naturaleza.[228] En este sentido en el caso "Mafiaboy" los ataques DDoS causaron daños económicos por más de mil millones de dólares por lo que, según Genosko, sus actividades podrían catalogarse tanto dentro del hacktivismo como del ciberterrorismo.

Por otro lado, estaban interpretaciones más optimistas como las de Naomi Klein (2000), quien consideraba los ataques como formas pacificas de hacking. De acuerdo con Klein las acciones de "Mafiaboy" reflejaban a un activista a favor de la libertad y parte del movimiento antiglobalización; en pocas palabras se trataba de la proyección de la comercialización de Internet. Sin embargo, el caso llevó a examinar los límites del hacktivismo como forma legítima de expresión, también provocó que las autoridades canadienses consideraran a la actualización del marco legal como un requisito urgente. De parte de ciudadanía fue evidente la incapacidad de la RCMP para identificar al culpable, y al mismo tiempo la sociedad civil comenzó a interesarse en el movimiento hacktivista.

Es preciso señalar que la actividad de Oxblood Ruffin en el ámbito hacktivista canadiense ha sido importante, pues junto a Paul Baranowski y el *Citizen Lab* de Toronto han unido esfuerzos a favor de la libertad de expresión en Internet tanto a nivel nacional como a nivel internacional. En especial se han enfocado en el desarrollo de software capaces de comunicar a las personas que viven en países donde la red está extremadamente controlada.

---

[226] Genosko, Gary. (2006). "FCJ-057 The Case of 'Mafiaboy' and the Rhetorical Limits of Hacktivism". *The Fibreculture Journal*, no. 9. [En línea]. Disponible en: <http://nine.fibreculturejournal.org/fcj-057/>. (Consulta 27/12/2013).

[227] Canadian Security Intelligence Service (1999). "Cyber-terrorism". [En línea]. Disponible en: <http://www.csisscrs. gc.ca/eng/operat/io2e.html>. (Consulta 27/12/2013).

[228] J. Paul B. De Taillon. (2001). *The Evolution of Special Forces in Counter-terrorism: The British and American Experiences.* Estados Unidos: Greenwood Publishing Group.

Al respecto, académicos como Ronald Deibert (director del *Citizen Lab*) consideran que el hacktivismo se ha convertido en una pieza fundamental para el desarrollo de la democracia en en el siglo XXI.[229]

De forma particular Ruffin se ha caracterizado por desarrollar múltiples programas informáticos a favor de los derechos humanos, desde 1999 demostró sus habilidades en este campo liderando una agrupación hacktivista que reunía a 30 programadores procedentes de diversos continentes.[230] Baranowski por su parte ha contribuido a la libertad de expresión a través del software *Sourcefabric* que ayuda al funcionamiento de los medios comunicación independientes ubicados en países donde el ejercicio periodístico puede ser censurado.[231]

Otro capítulo trascendente del hacktivismo en Canadá tuvo lugar durante las propuestas por la iniciativa C-309 (en 2012), la cual impone una condena hasta de diez años a los manifestantes que oculten su rostro; la iniciativa fue impulsada por Blake Richards (miembro del partido conservador); ante ello el grupo autodenominado *Anonymous*[232] hackeó sitios web del gobierno quebequense como forma de protesta.[233]

En cuanto a *WikiLeaks* para Stefania Milan y Arne Hintz (2013) el surgimiento del portal en la arena internacional ha transformado la percepción del hacktivismo. De acuerdo con Milan y Hinz después de la difusión de las filtraciones y tras la batalla legal que emprendió en diversas partes del mundo, *WikiLeaks* se transformó en el portavoz de la libertad de expresión en Internet, causando la movilización mundial de agrupaciones hacktivistas a favor de la divulgación de los cables y en defensa del portal.

Aunado a ello, Canadá se convirtió en uno de los objetivos predilectos del activismo en línea, especialmente después de intervención estadounidense en Iraq, pasando de 37 ataques en

---

[229] Shulgan, Christopher. (Diciembre 19, 2002). "Ottawa Citizen profile of the Citizen Lab and HACKTIVISM". *Citizenlab.* [En línea]. Disponible en: <https://citizenlab.org/2002/12/ottawa-citizen-profile-of-the-citizen-lab-and hacktivism/>. (Consulta 27/12/2013).

[230] *Ídem.*

[231] Kelly, Martina. (2013). "Paul Baranowski, Software Developer".*CareerMash.* [En línea]. Disponible en: <http:// careermash.ca/careers/meet-the-pros/paul-baranowski>. (Consulta 28/12/2013).

[232] Aunque inicialmente *Anonymous* no se consideraba un grupo hacktivista, con el paso del tiempo sus objetivos fueron incorporando demandas sociales, así como la elaboración críticas políticas, en busca de un sistema trasparente, donde los derechos a la información y a la libre expresión fueran respetados.

[233] LaSalle, LuAnn. (Febrero 13, 2013). "Hacktivists make their causes known online while masked in anonymity". *The Winnipeg Free* Press. [En línea]. Disponible en: <http://www.ctvnews.ca/sci-tech/hacktivists-make-their-caus es-known-online-while-masked-in-anonymity-1.1155160>. (Consulta 28/12/2013).

2002 a 459 en 2003, de acuerdo a un informe de la compañía *mi2g* (dedicada al desarrollo de prácticas y tecnologías para la gestión de riesgos globales). Los ataques aumentaron ante la posibilidad de que Canadá participara en la guerra; por esta razón ante la decisión de no enviar tropas a Medio Oriente el entonces Primer Ministro de Canadá Jean Chrétien confiaba que el número de ataques a los servidores nacionales se reduciría.[234] De este modo si adoptáramos la perspectiva de Dorothy E. Denning (2001), se confirmaría la influencia del hacktivismo en la construcción de la política exterior de los Estados-nación y en la percepción social de determinadas guerras.

En conclusión, es posible señalar que, si bien las TIC e Internet han colaborado al ejercicio activista, también se trata de una herramienta cuyos alcances y capacidad impulsarán la creación de medidas legislativas que regulen este tipo de prácticas en línea. El anonimato proporcionado por las redes puede ser un factor tanto a favor como en contra de las agrupaciones sociales. En adición, la frágil barrera entre ciberexpresión y vandalismo —reflejado en el caso "Mafiaboy"— dificultan la construcción de expectativas favorables para el hacktivismo. Sin embargo, existen logros considerables que no deben menospreciarse, el hecho de que expertos informáticos colaboren a la difusión de demandas sociales y faciliten herramientas para la movilización social, demuestra que un mundo globalizado también posee importantes beneficios. La percepción colectiva del derecho a la libre expresión y a la protección de los derechos humanos impulsa el intercambio de información e incentiva la transformación en naciones donde la democracia enfrenta grandes retos.

Canadá es sólo una muestra de lo que las nuevas tecnologías han generado en la sociedad, especialmente en un país que no requiere un cambio de régimen sino, más bien, de reforzar la democracia, convirtiéndola en un concepto lo suficientemente flexible como para admitir nuevas formas de participación, y de respetar el derecho a la información y a la libre expresión de la ciudadanía.

[234] Johnson, Ian. (Marzo 19, 2003). "Canada in hacktivist crosshairs".*The Globe and Mail.* [En línea]. Disponible en: <http://www.theglobeandmail.com/technology/canada-in-hacktivist-crosshairs/article1158937/>. (Consulta 28/12/2013).

4.3.3. La participación ciudadana a través de las TIC

De acuerdo con Pierre Levy (2004), cada día más usuarios de Internet —sin importar género, género, edad o estatus social— están informados sobre cuestiones políticas y participan en la democracia, ya que poseen mayor consciencia sobre su capacidad de acción en el ámbito político nacional y tienen más confianza en los procesos democráticos.[235] El incremento en el el grado de participación política puede deberse al aumento de información sobre dichos aspectos disponible en la red.

Al respecto una de las funciones de la red a favor de la participación ciudadana son los portales dedicados a promover el voto. En este sentido durante 1999 y 2000 se experimentó un crecimiento en el número de portales orientados a promover la democracia. Para Pierre Lévy (2004) la aparición de sitios electrónicos en beneficio de la sociedad está intrínsecamente relacionada con el surgimiento de un impulso democrático, que a su vez es producto de la adopción de nuevas tecnologías en el ámbito social. Para Lévy esta corriente democratizadora genera la necesidad de regímenes más transparentes e impulsa la creación de nuevos espacios de debate ciudadano. Los beneficios de la red se reflejan también en la aparición de portales sin ánimo de lucro, dedicados a difundir información política no partidista afín de incrementar el flujo de información en línea a favor de la ciudadanía.

Además la llamada "democratización de la información" ayuda a que los ciudadanos establezcan vínculos más cercanos con sus gobiernos. Por ello se puede afirmar que el arribo de las nuevas tecnologías en la esfera social trae consigo nuevas formas de colaboración en beneficio de la comunidad. Es importante señalar que la mayoría de estos proyectos surgen de asociaciones civiles preocupadas por la inclusión de la ciudadanía en el ejercicio político nacional.

Bajo otra perspectiva, es arriesgado sugerir que Internet ha provocado el desarrollo de una sociedad más participativa, y que ha despertado mayor interés en la actividad política nacional e internacional; puesto que podría ser que ese interés haya existido siempre sólo que no disponía de los medios adecuados para manifestarse.

---

[235] *Ciberdemocracia: Ensayo sobre Filosofía Política* (2004). Barcelona: Editorial UOC.

En cuanto a Canadá en diciembre de 2008 SC[236] publicó un estudio sobre la influencia de Internet en la convivencia social y política de la ciudadanía. El informe señala que las aplicaciones tecnológicas, específicamente la web, han transformado el comportamiento individual y colectivo de los ciudadanos, y que cuando se incorporan nuevas tecnologías a las formas de convivencia social surgen perspectivas tanto utópicas como distópicas; al respecto el análisis sugiere tres posibles transformaciones: aislacionismo, integración y la estructuración de redes complejas. En cuanto al impacto en las formas de convivencia es evidente la adopción de nuevas vías de comunicación, que en comparación con las formas tradicionales de convivencia, son más recurrentes en la vida cotidiana. Sin embargo, no es que las TIC estén desplazando el contacto personal, orientando a la sociedad a formas interacción exclusivamente cibernéticas, pues la web ha llegado a complementar los métodos de convivencia tradicionales; las nuevas tecnologías permiten establecer vínculos con individuos de diversas partes del mundo y con intereses específicos, a diferencia del siglo pasado cuando las relaciones sociales estaban determinadas por diversos factores como el geográfico.[237]

En pocas palabras se ha desarrollado nuevos procesos de cohesión social; por lo tanto los parámetros con los que solía calcularse el grado de participación ciudadana, pueden ser obsoletos cuando los aplicamos a la estructura social contemporánea.

A pesar de que Richard G. Niemi y Herbert F. Weisberg (2001) sostienen que existen evidencias sobre una disminución en la participación política en los últimos años, no significa que la sociedad canadiense actual sea menos activa que otras generaciones; más bien se trata de una transformación en las formas de participación. Anteriormente Niemi y Weisberg ya habían notado que la actividad ciudadana se estaba trasladando de métodos tradicionales, como el voto, a otros colectivos como protestas y manifestaciones.

Dado que la revolución electrónica es un fenómeno inconcluso —ya que la evolución de las comunicaciones es constante— es difícil determinar qué transformaciones sociales ha provocado. No obstante, periodistas como John Heilemann (2007) señalan que cada vez más

[236] Por sus siglas en inglés *Statistics Canada*, es una agencia del gobierno federal encargada de recoger y analizar datos estadísticos sobre Canadá y su población.
[237] Statistics Canada (Junio 12, 2008). *Canadian Internet Use Survey*. [En línea]. Disponible en: <http://www.statcan.ca/Daily/English/080612/d080612b.htm>. (Consulta 12/01/2013).

jóvenes están involucrados en actividades políticas de su país, pues el hecho de que la sociedad actual cuente con una gama más amplia de fuentes de información altera la naturaleza de la participación política ciudadana, ya que diversas y abundantes ofertas de información le facilitan mantenerse al tanto de cuestiones políticas, en adición el surgimiento de portales interactivos estimula el debate político a través del intercambio de opiniones.[238] Anteriormente la sociedad estaba limitada en la oferta informativa y debía conformarse con el contenido disponible en los mercados locales. En ese entonces las formas de expresión ciudadana se reducían al intercambio de correspondencia dirigida a funcionarios públicos o a periódicos sin la seguridad de recibir una respuesta. En este sentido anteriormente en Canadá la gama informativa variaba de acuerdo a la región; por esta razón la cantidad de fuentes disponibles dependía del tamaño del mercado, entre otros factores.[239]

Si se toma en cuenta que la información es un elemento que impulsa la participación social es posible determinar que gracias a la innovación tecnológica se han ampliado los medios informativos disponibles, y que también se les ha otorgado mayor accesibilidad y con ello se beneficiado a la participación ciudadana. De acuerdo con el diario *Toronto Star* el número de lectores se ha incrementado con la llegada de las plataformas electrónicas.[240] Según cifras de *Statistics Canada* la mayoría de los usuarios domésticos de Internet (67%) utilizaron la web para consultar noticias.[241] Además debido a que determinadas formas de participación (como las manifestaciones) son más comunes entre la población adulta, las TIC permiten que los jóvenes puedan participar bajo otras modalidades como en los foros en línea. De acuerdo con una encuesta general sobre el sector social (de 2003), aproximadamente un tercio de la población canadiense (33.2%) de entre 15 y 29 años utilizaron la web para informarse sobre cuestiones políticas; mientras que sólo un cuarto de la población (25.3%) de entre 30 y 49 años buscó información política en la red (véase tabla 6).[242] Aunado a ello, en los últimos años el

---

[238] Keown, Leslie-Anne (2007). "Keeping up with the times: Canadians and their news media diet." *Canadian Social Trends*, no. 82. [En línea]. Disponible en: <http://www.statcan.ca/bsolc/english/bsolc?catno=11-008-X200700396>. (Consulta 28/12/2013).

[239] Keown. *Óp. Cit.*

[240] Olive, David (Abril 8, 2007). "Rumours of newspapers' demise".*The Toronto Star*. [En línea]. Disponible en:<http://www.thestar.com/Business/article/200650>. (Consultada 13/08/2013).

[241] *Ídem.*

[242] Veenhof, Ben. *et.al.* (Diciembre 4, 2008). *How Canadians' Use of the Internet Affects Social Life and Civic Participation*. Statistics Canada. [En línea]. Disponible en: <http://www.statcan.gc.ca/pub/56f0004m/56f0004m2008016-eng.pdf>. (Consulta 28/12/2013).

porcentaje de hogares con acceso a Internet ha incrementado, en 2012 el 83% de los hogares canadienses tenía acceso a Internet, por lo que el número de búsquedas de información en la web también podría haber aumentado.[243]

Tabla 6. Porcentaje de usuarios domésticos de Internet* que usan la web para leer e intercambiar información sobre cuestiones sociales o políticas en Canadá (2005).

	Leen periódicos en línea o revistas determinadas cuestiones sociales o políticas	Leen lo que otros canadienses piensan sobre determinadas cuestiones sociales o políticas	Coinciden con otros canadienses sobre determinadas cuestiones sociales o políticas
	% de usuarios domésticos de Internet		
TOTAL	51.4	29.2	13.8
Sexo			
Masculino	57.8	35.2	17.2
Femenino	45.1	23.3	10.5
Edad			
18 a 24	58.3	35.4	21.3
25 a 34	56.7	33.7	13.8
35 a 44	50.2	27.6	11.7
45 a 54	48.1	27.0	11.0
55 a 64	45.5	24.0	13.1
65 y mayores	40.7	20.6	13.1 [t]
Nivel académico			
Menor a Secundaria	37.2	18.2	7.3 [t]
Otros estudios Medio superiores	44.0	23.0	10.2
Certificado o equivalente de nivel superior	54.9	34.1	18.8
Título Universitario	48.1	24.5	11.3
Localidad	63.1	40.5	19.4
Urbana	53.2	30.5	14.4
Rural o pequeñas poblaciones	43.8	24.0	11.6

[t] – uso con asistencia

*– Esta tabla incluye individuos mayores de 18 años que declararon haber usado Internet desde casa para uso personal en los 12 meses anteriores a la encuesta.

Fuente: *Statistics Canada*, Canadian Internet Use Survey, 2005.

En 2006 un estudio general que mide el nivel de alfabetización y habilidades de la población adulta en Canadá reflejó que los usuarios regulares de Internet son más propensos

[243] Statistics Canada. (Noviembre 26, 2013). *Canadian Internet Use Survey, 2013*. [En línea]. Disponible en: <http://www.statcan.gc.ca/daily-quotidien/131126/dq131126d-eng.pdf>. (Consulta 11/05/2014).

a involucrarse en actividades políticas, que aquellos que no utilizan la red.[244] Para George Sciadas (2006) director adjunto de *Statistics Canada*, la Sociedad de la información además de de estar interesada en consultar datos, también ha demostrado ser muy participativa. Por otro lado es posible determinar que la estructura de la sociedad se ha vuelto más compleja, y que Internet no ha disminuido la participación social, al contrario le ha otorgado nuevos medios para compartir su opinión a un mayor número de personas.

En este sentido *WikiLeaks* no aparece como un agente transformador de la actividad política canadiense, sino como una consecuencia de la incorporación de las nuevas tecnologías en la vida social y política de ciudadanía; demuestra lo que las plataformas electrónicas pueden hacer a favor de la democracia y de la libertad de información, dado que promueve los conceptos de transparencia en las estructuras estatales y la participación social.

Por último, es necesario señalar que la opinión pública respecto a *WikiLeaks* en Canadá es menos radical que en Estados Unidos, pues de 1000 estadounidenses encuestados 51% rechaza las acciones de *WikiLeaks* y sólo un 19% las apoya; en contraste de 1005 canadienses 36% condena las publicaciones y 30% expresa su apoyo a la organización. Por otra parte el 61% de los canadienses encuestados considera que las filtraciones podrían dañar las relaciones del país con Washington.[245] Como se ha observado la percepción del fenómeno *WikiLeaks* en Canadá es diversa lo que, sin duda, se debe al apoyo que grupos activistas brindan a la organización; en adición, la sociedad canadiense también posee un alto grado de consciencia sobre los alcances de las nuevas tecnologías tanto en el plano nacional como en el internacional.

4.4. El impacto en los medios de comunicación

Los medios de comunicación representaron un elemento esencial para la proyección internacional de *WikiLeaks*. No obstante, dentro de la esfera periodística hay tanto facciones a favor como en contra de la organización. No es extraño encontrar dentro del ámbito informativo quienes consideran a *WikiLeaks* como un desafío, ya que ha llegado a transformar

---

[244] Veenhof, Ben. (Mayo 15, 2006). *Determinants and Outcomes of Heavy Computer Use: An International and Interprovincial Comparison.* Presentación de *Statistics Canada* en la Conferencia Socio-económica de Gatineau, Quebéc.

[245] Angus Reid Public Opinion. (Diciembre 9, 2010). *Half of Americans Condemn WikiLeaks. Release; Britons and Canadians Split*. Vision Critical. [En línea]. Disponible en: <http://www.angusreidglobal.com/wp-content/uploads/2010/12/2010.12.09_WikiLeaks.pdf>. (Consulta 28/12/2013).

los alcances de las filtraciones periodísticas con el uso de nuevas vías de comunicación, pero también están los que apoyan su labor y resaltan sus aportaciones en cuestiones como el derecho a la información y a la libre expresión. En este sentido un buen ejemplo es el trabajo realizado por Michael Geist, doctor en Derecho, y colaborador de los diarios *Vancouver Toronto Star* y *The Ottawa Citizen*. Geist a través de diversas columnas y de un blog se ha dedicado a analizar las filtraciones relacionadas con el Acuerdo de Asociación Transpacífico y su impacto tanto en la sociedad como en la legislación canadiense.[246]

Por otra parte, están aquellos que no consideran importante el trabajo de la organización y tampoco lo consideran parte del periodismo. Al respecto Joshua Noble colaborador de *The Toronto Star* cuestiona si *WikiLeaks* puede ser reconocido como una forma ética de hacer periodismo y sostiene que la organización no midió el alcance del daño provocado por las publicaciones.[247]

Dado que *The Toronto Star* también se ha dedicado a profundizar en la vida del Editor en jefe de la organización Julian Assange[248] el diario *Huffinton Post* ha declarado que los medios dominantes en Canadá se esfuerzan por desvirtuar la importancia de los cables, prestando mayor atención al medio que al mensaje, formando parte de la táctica occidental para dañar la reputación de *WikiLeaks*.[249] En medio de estas discusiones aparecen opiniones como la de Jordan Benjamin Press de *Queen´s University* cuya posición es más neutral, ya que reconoce el derecho a la información por parte de la ciudadanía; sin embargo aclara que debe ser utilizada de forma responsable.[250]

---

[246]Geist, Michael. (2008-2013). *WikiLeaks*. [Blog]. Disponible en: <http://www.michaelgeist.ca/index.php?option=com_search&Itemid=99999999&searchword=WikiLeaks&searchphrase=any&ordering=newest&limit=50&limitstart>. (Consulta 23/01/2014).

[247] Noble, Joshua. (Junio 2, 2011). "WikiLeaks, Canadian media and democracy: Media with a face". *The Toronto Star*. [En línea]. Disponible en: <http://www.thestar.com/opinion/editorialopinion/2011/06/02/wikileaks_canadian_media_and_democracy_media_with_a_face.html>. (Consulta 27/01/2014).

[248] Carter, Matt. (Diciembre 1, 2010). "10 things you don't know about WikiLeaks mystery man Julian Assange". *The* Toronto *Star*. [En línea]. Disponible en: <http://www.thestar.com/news/world/2010/12/01/10_things_you_dont_know_about_wikileaks_mystery_man_julian_assange.html>. (Consulta 26/01/2014).

[249] Arar, Maher. (Diciembre 14, 2010). "Enough Hypocrisy: WikiLeaks Is Filling a Vacuum". *The Huffington Post*. [En línea]. Disponible en: <http://www.huffingtonpost.com/maher-arar/enough-hypocrisywikileak_b_796238.html>. (Consulta 24/01/2013).

[250] Benjamin Press, Jordan. (2011). *NEWS YOU CAN REALLY USE: Thoughts from Ontario journalists about the what and how of teaching news literacy*. (Tesis de Maestría). Queen's University. Ontario. [En línea]. Disponible en: <http://qspace.library.queensu.ca/bitstream/1974/6414/1/Jordan%20Press%20Thesis.pdf>.

El debate canadiense en torno a *WikiLeaks* oscila entre, si ha llegado a romper el modelo en donde los periodistas tenían el derecho, casi exclusivo, a acceder a la información en bruto, o si las filtraciones han generado un beneficio, o bien, un problema a la sociedad y a los medios de comunicación, pues es evidente que con la publicación de las filtraciones se implementarán normas más restrictivas, tanto para el flujo de Internet como para el contenido de los medios.

En síntesis, *WikiLeaks* revalida la transformación de los medios tradicionales que comenzó a experimentarse desde finales del siglo pasado. En este contexto los medios de información y especialmente la prensa preservan su importancia dentro de la democracia; hoy más que nunca, ante la abundancia de información disponible en la red, los medios deben elaborar análisis críticos que contribuyan a la construcción de una sociedad más justa.

Si bien *WikiLeaks* ha generado diversas posturas dentro del periodismo canadiense no se trata de reemplazar a la prensa tradicional con plataformas cibernéticas, sino de ofrecer nuevos instrumentos y nuevas fuentes de información, que junto a las formas convencionales de hacer periodismo establezcan un equilibro, evitando caer extremos como: publicaciones masivas de datos en bruto (sin ningún tipo análisis), y que no aportarían nada bueno a la sociedad; o en la sobrevaloración de los medios tradicionales como única fuente de información efectiva. Esta situación constituye un desafío para los medios canadienses; sin embargo, es probable que ese equilibrio se consiga en la marcha, y en la medida en la que uno y otro lado —los medios tradicionales y los electrónicos— aprendan de sus errores y adopten aquellas herramientas que una y otra parte pueden proporcionar al ejercicio de un periodismo apropiado para la Sociedad del conocimiento.

4.5. Retos y perspectivas

El surgimiento de *WikiLeaks* en la dinámica internacional ha llevado a considerar el potencial moderno de las filtraciones periodísticas también ha dirigido la atención hacia el ciberespacio, que al constituir un nuevo espacio de interacción influye también en diversos ámbitos como en el social, económico y político. En este aspecto la red representa una cuestión compleja para los mecanismos de control del Estado, y para el ejercicio de su soberanía.

(Consulta 12/01/2014).

Por otra parte, la revolución tecnológica ha trasladado las libertades convencionales a una dimensión cibernética, donde aparecen los llamados "derechos digitales". Es decir ejercicios como la participación ciudadana, el derecho a la información, la transparencia institucional, entre otros persisten en la "aldea digital", donde su alcance y contenido es mayor. Por ello en los últimos años las naciones se han esforzado por modernizar el funcionamiento de las estructuras estatales; incluir a la sociedad en la esfera digital, y estructurar las medidas adecuadas para proteger los sistemas cibernéticos nacionales. Sin embargo, el incesante avance tecnológico junto a la existencia de una brecha digital ha creado desafíos para las autoridades tanto a nivel nacional como a nivel internacional.

Entre las dimensiones más importantes de esta nueva realidad está la construcción de un gobierno electrónico eficiente; el establecimiento de normas orientadas a la rendición de cuentas y al acceso a la información de carácter público; la creación de canales eficaces de comunicación con la ciudadanía, y la instauración de medidas legislativas que procuren la protección y regulación de Internet sin afectar los derechos de la ciudadanía.

Por lo anterior es preciso analizar los retos y las perspectivas del gobierno canadiense en su búsqueda por un gobierno electrónico y por la regularización de Internet.

4.5.1. El *e-government* canadiense

Dado que la sociedad informática se desenvuelve en un entorno donde los datos son un elemento abundante y el ciberespacio el soporte central, la ciudadanía contemporánea requiere de mecanismos de gobernanza capaces de integrase a esta nueva dinámica.

En la actualidad las oportunidades de comunicación con el Estado se han ampliado y diversificado debido a que la sociedad ha incorporado exitosamente el uso de las TIC a la vida cotidiana, como consecuencia desean utilizar también estos medios en los procesos de interacción con el gobierno. Es por esta razón que las naciones requieren de mecanismos más eficaces y flexibles que los vinculen eficazmente con la ciudadanía.

Durante los últimos años Canadá ha estado consciente de la importante función que desempeñan las TIC en el mundo, y reconoce que su inserción en el funcionamiento del gobierno debe ser un objetivo esencial.

Al respecto desde finales del siglo XX comenzó a desarrollarse el concepto de *e-government* o gobierno electrónico que, de acuerdo con Don Tapscott y David Agnew (1999), se refiere a un modelo de gobernanza con mayor base comunitaria y mayor conectividad gracias a las facilidades que otorga el uso de nuevas tecnologías.

Canadá fue una de las primeras naciones en adoptar el modelo de gobierno electrónico. En octubre 1999 estableció el objetivo de convertirse en el líder mundial en el uso de nuevas tecnologías. Para lo cual ha determinado las siguientes metas: reducir los costos de los servicios de información y de los trámites ciudadanos; brindar acceso total a la población sin importar lugar y hora; agilizar tanto el manejo de datos como la gestión de trámites, e implementar mecanismos de seguridad capaces de proteger las plataformas cibernéticas nacionales.[251] Sin embargo, con la expansión de las nuevas tecnologías Canadá se ha enfrentado a diversos retos que demandan la constante actualización de las estrategias nacionales para un gobierno electrónico y que también ponen a prueba la cooperación entre autoridades locales, provinciales y federales.

Con el deseo de convertirse en el país más conectado del mundo Canadá desarrolló diversos programas para facilitar las conexiones nacionales e internacionales, y optimizar la función de las instituciones públicas y privadas a fin de ampliar el potencial económico y político de la nación. Progresivamente ha creado planes de financiación de proyectos tecnológicos a nivel provincial, se ha preocupado por extender el servicio de banda ancha a las comunidades que más lo necesitan, y ha establecido puntos de acceso público en diferentes áreas del territorio.[252] No obstante, existen características sociales que el gobierno canadiense no tomó en cuenta, como la adaptación de la ciudadanía a los nuevos medios, y la diversidad social en cuestiones culturales y de edad. Aunado a esto las diferencias económicas entre localidades hicieron que el acceso a la información se convirtiera en un recurso exclusivo para aquellos que contaran con equipos electrónicos y acceso a Internet.

La coordinación de esfuerzos hacia un gobierno electrónico también puso en evidencia la compleja interacción entre niveles gubernamentales, pues las provincias y autoridades locales

---

[251] Fraser, Charmaine. (2009). "E-Government: The Canadian Experience".*Dalhousie Journal of Interdisciplinary Management*, vol. 4, pp. 1-14. [En línea]. Disponible en: <http://djim.management.dal.ca/issue_pdfs/Vol4/Fraser_The_Canadian_Experience.pdf>. (Consulta 24/01/2014).

[252] *Ídem.*

requerían de autoridad legislativa y ejecutiva para implementar medidas ajustadas a cada región. Sin embargo, existieron mecanismos exitosos como *Smart Communities Program* (implementado de octubre de 2000 a septiembre de 2003), el cual destinó 60 de dólares del gobierno federal para financiar 10 proyectos provinciales (más uno en zona indígena y otro más en el área norte) que tenían como objetivo mejorar la oferta de los servicios en línea. Con dicho programa además de apoyar las iniciativas provinciales se buscaba aprender de la experiencia y otorgar oportunidades de negocio a nivel nacional e internacional a las provincias.[253]

Una de las observaciones hacia *Smart Communities Demonstration Program* es que no impulsa la participación ciudadana y la democracia, de esta forma el desarrollo de dichas cuestiones quedaba en manos de las autoridades provinciales y locales, para Collins (*et al.*2002) esta tendencia no es sorprendente si se toma en cuenta el modelo nacional basado en el sistema *Westminster* que es poco compatible con el modelo descentralizado y de mayor participación como lo es la naturaleza de la interacción en Internet.[254]

De acuerdo con Barnet (1997), el arraigo a los viejos modelos de acción económica y política dificulta el desarrollo de estos sectores en el ciberespacio. Barnet ubica entre los desafíos del gobierno canadiense la colaboración multinivel y, en especial, la creación de mecanismos para que el gobierno federal facilite las tareas de las autoridades locales. Sin embargo, la iniciativa canadiense hacia un modelo de gobernanza electrónica es importante porque es vista como un instrumento para mejorar el liderazgo y competitividad tanto a nivel interno como externo. Empero, los desafíos persisten, es evidente la dificultad en la coordinación y seguimiento de los programas para mejorar el uso de aplicaciones tecnológicas a nivel nacional. Según *Accenture* (empresa dedicada a servicios de consultoría) en 2005 40% de los canadienses eran optimistas con respecto al uso de las TIC

[253] Collins, Bill; Paquet, Gilles; Roy, Jeffrey y Chris Wilson. (Mayo 10-11, 2002). E-Governance and Smart Communities: A Social Learning Challenge. En *SSHRC Knowledge Based Economy*. Conferencia llevada a cabo en Memorial University of Newfoundland, St. John's, Newfoundland. [En línea]. Disponible en: <http://www.christopherwilson.ca/papers/Nfld_paper_2002.pdf>. (Consulta 25/01/2014).
[254] *Ídem.*

en los servicios gubernamentales;[255] no obstante en 2006 tres cuartas partes de la población expresó preocupación por la seguridad de sus datos.[256]

Dado que en los últimos años Canadá ha perdido liderazgo en el desarrollo del *e-government government* se requiere de medidas estratégicas capaces no sólo de cubrir las necesidades específicas de cada región, sino de dar seguimiento a la implementación de programas y de otorgar un lugar importante a la percepción social de dichas medias, lo cual representa un panorama complejo, pues se deben tomar en cuenta cuestiones como los fondos necesarios para para dicha tarea (además de estructurar mecanismos efectivos de rendición de cuentas). Por otro lado el principal reto para mantenerse como uno de los países más conectados del mundo es conservar la importancia del *e-government* en la administración actual, ya que la mayoría de los programas se estructuraron y aplicaron cuando el partido liberal ocupaba el poder, por lo que las prioridades políticas se trasformaron con la llegada de Stephen Harper,[257] es preciso que este y otros programas mantengan importancia y se les dé seguimiento, pues los beneficios adquiridos van más allá de victorias partidistas, ya que se trata de la competitividad de la nación.

4.5.2. La transparencia institucional

Cuando Canadá estructuró la estrategia de gobierno electrónico consideró a la accesibilidad y a la participación ciudadana como elementos fundamentales. Sin embargo, no sólo se trata de facilitar el uso de nuevas tecnologías e incentivar la participación social, pues la transparencia institucional surge como eje central en el camino hacia un *e-government* efectivo.

Giovanni Ziccardi (2013) señala que la percepción contemporánea de "transparencia" contempla a las estructuras gubernamentales como plataformas para la difusión de datos y servicios. En este sentido los programas estatales ocupan un papel importante en la construcción de formas más democráticas y participativas de gobierno.

---

[255] Accenture. (2005). *Leadership in customer service report: New expectations, new experiences*. [En línea]. Disponible en: <https://www.accenture.com/Global/Research_and_Insights/By_Industry/Government_and_Public_Service/default.htm>. (Consulta 23/11/2013).

[256] Statistics Canada. (2006). *The daily: Canadian Internet use survey*. [En línea]. Disponible en: <http://www.statcan.gc.ca/daily-quotidien/060815/dq060815b-eng.htm>. (Consulta 15/01/2014).

[257] Accenture. (2007). *Leadership in customer service: Delivering on the promise*. [En línea]. Disponible en: <https://www.accenture.com/Global/Research_and_Insights/By_Industry/Government_and_Public_Service/default.h>. (Consulta 20/12/2013).

De acuerdo con Ziccardi dentro de esta nueva dinámica la sociedad emerge como el actor principal, al que se le proveerán las vías y mecanismos necesarios para acceder libremente a la información relacionada con las funciones del Estado.

Dicha interpretación resulta comprensible si se toma en cuenta que el flujo de información en el sector social ha incrementado de forma importante con el uso de Internet y con la aplicación de nuevas tecnologías; en adición las redes de interacción se han expandido, traspasando los límites estatales. Por ello si las conexiones entre individuos se han facilitado e incrementado con el uso de las TIC es evidente que la ciudadanía, además de demandar un grado semejante de interacción con las autoridades exija también mayor transparencia.

Por su parte los Estados pueden aprovechar esta tendencia para mejorar la percepción de la ciudadanía. En los últimos años diversas naciones alrededor de mundo han buscado mejorar su imagen nacional e internacional a través del establecimiento de estrategias de apertura y transparencia en las estructuras gubernamentales.

Particularmente las instituciones canadienses se han dedicado a analizar los efectos que la transparencia y la confianza provocan en los organismos estatales. Este estudio también se ocupa de las formas en las que el ciberespacio facilita el dialogo y la difusión de información (y de conocimiento) por todo país. Por su parte los organismos dedicados al servicio público también se han interesado por los efectos de las TIC y declaran que la democracia representativa en Canadá no está siendo reemplazada, sino al contrario se está volviendo más participativa.[258]

En la esfera política también hay quienes se han dedicado a promover los beneficios de Internet, por ejemplo el ex presidente del Consejo del Tesoro (bajo el gobierno de Paul Martin) Reg Alcock se ha pronunciado a favor de nuevas formas de participación; sin embargo, Alcock también ha reconocido que será difícil transformar las estructuras gubernamentales. En 2004 el entonces Primer Ministro, Paul Martin, intentó impulsar reformas orientadas a ampliar la participación democrática, aunque obtuvo logros parciales encontró escaso interés político en el asunto, por lo que sus objetivos no prosperaron.

[258] Joy, Jeffrey. (2006). *E-government in Canada: Transformation for the Digital Age*. Canada: University of Ottawa Press.

Aunque la esfera política canadiense sigue mostrando interés por incrementar la participación política ciudadana e impulsar la democracia electrónica no existe una orientación clara al respecto. Jeffrey (2006) también establece cuatro desafíos para Canadá en este aspecto: 1) la secrecía operacional inherente a los esfuerzos de las reformas internas y la falta de compatibilidad entre las agendas de seguridad y los programas de impulso a la participación democrática; 2) las debilidades en el manejo de información por parte del gobierno federal y su resistencia a una mayor apertura; 3) el carácter contradictorio de los procesos parlamentarios actuales, y 4) la ausencia de mecanismos que compartan el estado de las negociaciones y la existencia de instrumentos políticos de gestión de información en función de quienes tienen la autoridad.

A pesar de estas dificultades en 2011 el gobierno canadiense presentó un nuevo plan de acción hacia un gobierno abierto donde señala que el país mantiene su compromiso por la rendición de cuentas y por el impulso a la participación ciudadana, lo importante en esta iniciativa es que se consultó a la ciudadanía con el objetivo de tomar en cuenta sus expectativas en la creación del programa. El uso de las nuevas tecnologías es uno de los ejes sobre los que se desarrolla este plan (véase figura 5). Aunado a ello Canadá ha buscado la colaboración de entidades internacionales para optimizar la transparencia institucional, actualmente trabaja con *International Aid Transparency Initiative* la cual colaborará en la mejora de los instrumentos de transparencia y ofrecerá reportes públicos sobre la evolución de Canadá en este aspecto.[259]

[259] Government of Canada. (Enero 8, 2013).*Canada's Action Plan on Open Government.*Data.gc.ca. [En línea]. Disponible en: <http://data.gc.ca/eng/canadas-action-plan-open-government#toc2>.(Consulta 26/01/2014).

Figura 5. Compromisos canadienses hacia un gobierno abierto

Fuente: Government of Canada (Enero 8, 2013). *Canada's Action Plan on Open Government*. Data.gc.ca. [En línea]. Disponible en:<http://data.gc.ca/eng/canadas-action-plan-open-government#toc2>.

Es importante señalar que el plan presentado en 2011 se aplicará a lo largo de 3 años, por lo que sus resultados se conocerán, por lo menos, hasta 2015. Sin embargo, el hecho de que Canadá haya buscado colaboración internacional en esta materia es un punto importante, y que sin duda incrementará la confianza de la ciudadanía respecto al compromiso del gobierno en la búsqueda de mejores resultados.

Empero, bajo la perspectiva de las provincias Canadá no ha aprovechado al máximo las oportunidades que ofrecen las TIC para difundir información gubernamental, también señalan que la mayoría de la atención se centra en la mejora de los servicios públicos.

De forma particular Ontario declara que una sociedad informada es un elemento fundamental para la implementación del *e-government*. El Comisionado para la Información y la Privacidad (de Ontario) propone tres trasformaciones para promover la trasparencia a través de la difusión electrónica de información: la primera es un cambio de enfoque donde los mecanismos de rendición de cuentas ocupen el lugar central; segundo, modernizar la gestión de datos y facilitar el acceso a la información, y el último, mejorar la capacidad

estatal para cubrir las demandas de información de la ciudadanía mediante la adquisición y desarrollo de aplicaciones tecnológicas. Para Ontario el gobierno es la entidad con mayor base documental, por lo que tiene la obligación de ofrecer acceso tanto a los datos actuales como a los históricos. Desde esta perspectiva en el marco de una "economía del conocimiento", donde los datos han desplazado a los bienes materiales como única fuente de bienestar, el papel de Estado como difusor de información se ha profundizado. Por otra parte si bien las TIC han aumentado la capacidad de acción de los ciudadanos, es necesario que éstos estén mejor informados acerca de la estructura y el funcionamiento de sus instituciones para participar de forma efectiva.[260]

Para finalizar es preciso señalar que los esfuerzos canadienses a favor de la transparencia son significativos, pues en comparación con otros países ha demostrado mayor interés en esta cuestión. Sin embargo, la complejidad social y política de la nación demanda la modernización constante de estos mecanismos. Retomando a Roy Jeffrey (2006) no son suficientes los mecanismos para la rendición de cuentas cuando lo que hace falta es voluntad política; probablemente esto se deba a que la propuesta de mayor participación ciudadana se enfrente con la esencia de la estructura política canadiense; no obstante, en plena Era del conocimiento la sociedad no debe ocupar el mismo lugar que en el siglo XX. Impulsar normas de transparencia institucional en un sistema político (y administrativo) cerrado es por demás obsoleto. Rieg Alcock ya había señalado que la trasformación de las bases nacionales sería difícil, y quizá éste sea el reto más grande que enfrenta Canadá. El desafío consiste en impulsar mecanismos modernos de interacción ciudadana en un entorno que, en esencia, ha permanecido estático. Para Canadá como para muchas otras naciones reconocer el empoderamiento de la ciudadanía es un asunto complejo. No obstante, la sociedad contemporánea ha ampliado (y continuará haciéndolo) la demanda de información y la intolerancia al secretismo. El surgimiento una sociedad informada, deseosa por formar parte de los debates políticos e interesada en el funcionamiento de las estructuras gubernamentales siempre será un factor en beneficio de la nación.

[260] Cavoukian, Ann y Tom Mitchinson. (Abril, 2011).*Promoting Transparency through the Electronic Dissemination of Information*. Information and Privacy Commissioner/Ontario. [En línea].Disponible en: <http://www.ipc.on.ca/i mages/resources/up-protrans.pdf>.(Consulta 28/01/2014).

4.5.3. Expectativas de la participación política ciudadana en el ciberespacio

Como se ha observado el aumento en la cantidad de información disponible y la adopción de nuevas vías de interconexión han repercutido en el sector social. De manera que si consideramos el concepto de participación política de Hannah Arendt (1958) entendiéndolo como una acción colectiva en busca de justicia pública a través del pensamiento racional y de acciones prácticas, es posible interpretar que las TIC han ampliado los elementos informativos necesarios para ese pensamiento y que las modalidades de acción práctica se han multiplicado.

Esta transformación puede ser vista desde diferentes enfoques como el de Darin Barney (2003) quien sugiere que las TIC no han generado una nueva etapa en las formas de participación ciudadana. Barney también sostiene que la esfera pública ha sido invadida por la ideología mercantilista contenida en Internet, por lo que el razonamiento crítico ha sido desplazado de la opinión pública. Desde esta visión las TIC no están a favor de la ciudadanía, más bien forman parte de una etapa en la evolución social, y la web por su naturaleza está condenada a servir a los intereses capitalistas.

No obstante, a pesar de esta confrontación de ideas es un hecho que durante los últimos años Canadá y diversos gobiernos de todo del mundo han integrado, poco a poco, al sector social en diversas dinámicas estatales a fin de ampliar e incentivar su participación en los procesos de estructuración de normas y en los debates políticos. Sin embargo, las estrategias canadienses han prestado mayor atención a la propagación de las TIC en la población, y a la incorporación de nuevas plataformas en la estructura estatal, descuidando el punto de la participación ciudadana, que de por sí es un tema difícil de abordar, ya que la propuesta de otorgar mayores atribuciones a la sociedad en el ejercicio político no es una decisión fácil para cualquier Estado. Empero, Internet se ha convertido en un foro multilateral en donde la naturaleza de los procesos de interacción (horizontal y multicanal) hace que la idea de una jerarquía estricta resulte inadmisible.

El punto crítico en este aspecto es el potencial democrático que poseen los medios de comunicación, de acuerdo con Jürgen Habermas (1987). En este sentido el régimen de monarquía parlamentaria federal puede sentirse amenazado. Jeffrey Roy (2006) señala que

el Parlamento canadiense ya no es supremo, pues el potencial del que habla Habermas le ha otorgado mayor protagonismo a la acción ciudadana. De acuerdo con Roy el papel del Parlamento (o de las legislaturas provinciales) como mecanismo para procurar el buen funcionamiento del gobierno a favor del bienestar común, debe amoldarse a las nuevas formas de interacción social; si bien es necesario promover la transparencia y la rendición de cuentas, es preciso procurar también la participación ciudadana, ya que funciona como agente legitimador de las actividades gubernamentales.

En síntesis el papel de la ciudadanía como monitor de las decisiones políticas y legislativas de las autoridades se ha reforzado gracias a la revolución tecnología; en suma la evolución hacia nuevas formas de interacción no parece una decisión opcional sino obligatoria, puesto que la cooperación internacional en esta materia ha aumentado de forma importante. El surgimiento de organizaciones interestatales que procuran la rendición de cuentas, evalúan la efectividad de los gobiernos, difunden y protegen los derechos civiles, etc., es un aporte importante para la evolución de las naciones y para el bienestar de la sociedad. Al respecto la publicación de estudios que revelan qué países son líderes en la promoción y respeto de la participación social, confirma que la opinión pública posee mayor peso (ejerciendo presión para que los países implementen los mecanismos correspondientes).

En Canadá la compleja estructura social hace que las estrategias orientadas a la participación ciudadana queden en manos de autoridades locales, ya que ellos (mejor que cualquier otra estructura) conocen los requerimientos especiales para que la población pueda adoptar nuevos canales; no obstante, es necesario desarrollar vías de comunicación directa con las instituciones federales, ya que finalmente son quienes poseen mayor autoridad en determinadas cuestiones.

Roy Jeffrey también afirma que la tendencia histórica del Estado respecto a la ciudadanía ha sido colocar mayor cantidad de información pública en línea, por lo que los recursos destinados a promover la participación pública han sido menores.

El panorama en esta cuestión resulta interesante, pues las medidas que implemente Canadá en este aspecto determinarán un nuevo rumbo en la actividad política canadiense. Si bien, se ha consultado a la ciudadanía en la estructuración de determinadas estrategias, se requieren de canales interactivos que impulsen el intercambio de información en doble vía, y que los

portales web y otros mecanismos estatales no se queden sólo en el papel de expositores de información. La naturaleza política canadiense puede ser una barrera difícil de derribar; sin embargo, la tendencia mundial hacia una mayor participación (proyectada con la aparición de organismos internacionales, ONG y asociaciones civiles) son un elemento a favor de la ciudadanía. Puesto que la sociedad canadiense es rica en diversidad cultural e ideológica mantener un muro contra la participación ciudadana será difícil de sostener. Queda en las manos del gobierno mantener esta muralla o crear espacios donde la opinión de la mayoría no sólo sea escuchada sino tomada en cuenta.

4.5.4. Reformas políticas orientadas a la regulación de Internet

Cuando se habla de la regulación de Internet no se hace referencia al control de un determinado sector de la sociedad sino de regular todo un conjunto de actividades sociales que se llevan a cabo en un espacio virtual. La red se ha convertido en un lugar donde se llevan a cabo tanto transacciones financieras, como prácticas de mercado, campañas políticas, manifestaciones sociales, conferencias académicas, etc. Por esta razón hablar de una sola regulación es complicado.

El establecimiento de normas para el control de contenido o de tráfico de Internet; para la protección de derechos de autor o de infraestructuras nacionales, etc. significa un gran reto. Además se debe considerar que la web está conformada por múltiples organizaciones que trabajan en conjunto para establecer estándares de interoperabilidad.[261]

En Canadá los proveedores de servicios de Internet, ISP (por sus siglas en inglés), tienen la facultad de negar acceso y censurar contenido en la web, lo cual evidentemente ha provocado inconformidad. Como consecuencia académicos como Jeff Miller (2012) han hecho un llamado para la neutralidad de Internet, también diversas organizaciones civiles participan en la promoción de mejores normas, preocupándose por proteger los derechos civiles.

[261] Miller, Gerry; Sinclair, Gerri; Sutherland, David y Julie Zilber (Marzo, 1999). *Regulation of the Internet. A technological Perspective*. Spectrum Management and Telecommunications. [En línea]. Disponible en: <http://www.ic.gc.ca/eic/site/smt-gst.nsf/vwapj/05082-eng.pdf/$FILE/05082-eng.pdf>. (Consulta 28/01/2014).

Si bien el gobierno canadiense a través de la Comisión de Radio-televisión y Telecomunicaciones ofrece un espacio para atender las denuncias ciudadanas sobre la gestión de los ISP, el control del tráfico en línea debería contar con la participación de autoridades estatales; recientemente han surgido reclamos en contra de la intervención de los proveedores en el contenido del tráfico de datos, al respecto Miller señala que aunque es necesario actualizar determinadas normas para abarcar esta práctica, la ley de telecomunicaciones ha establecido en su sección 23 que ningún operador de infraestructura puede intervenir el contenido.

Sin embargo, esta postura suele enfrentarse con la protección a la propiedad intelectual, que como se ha observado tanto en el plano nacional como en el internacional constituye un tema sensible.

Si bien se han presentado iniciativas y propuestas de reforma en telecomunicaciones, la polémica surge cuando se analiza la extensión de dichos instrumentos principalmente cuando las actividades de los usuarios podrían ser monitoreadas e incluso cuando se podría acceder a datos personales; empero existen normas exitosas que han permitido perseguir y sancionar actividades como el fraude en Internet, el comercio ilegal y la pornografía, que demuestran el interés y efectividad de las autoridades federales y provinciales.

El panorama canadiense hacia la regulación de Internet requiere de la apertura de un foro nacional donde tanto asociaciones civiles como la ciudadanía, proveedores de Internet y los diferentes niveles de gobierno establezcan directrices capaces de proteger los derechos y libertades de cada elemento. La normativización también demanda seguridad de que cada una de las partes cumplirá lo establecido, requiere de compatibilidad legal para cada localidad o provincia, y dela infraestructura e instrumentos adecuados.

Para concluir, es preciso señalar que Internet constituye por sí misma un reto significativo, pues se trata de un lugar intangible; de una enorme red de autopistas virtuales que trasladan millones de paquetes información de un lugar a otro en cuestión de segundos y sin fronteras. Se trata de un medio que ha permitido la propagación de información, e interconectividad más gran de la historia donde convergen tanto grupos activistas como organizaciones terroristas; se trata del más importante desafío legal para los aparatos jurídicos nacionales, y principalmente

para la autoridad del Estado. Empero, en este como en otros retos la cooperación ocupa el lugar central, quizá en la actualidad la jurisdicción en Internet parezca frágil todavía, pero con el paso del tiempo se localizaran debilidades y se implantarán mejores prácticas hacia una regulación eficiente. El fenómeno *WikiLeaks* revivió la importancia de este aspecto y provocó que las nociones de gobierno electrónico, trasparencia, participación ciudadana, derecho a la información y la interacción gobierno-sociedad fueran nuevamente analizadas. Desde distintas perspectivas puede verse como un desafío a la protección de sistemas y comunicaciones nacionales o como la confirmación del poder de la ciberefera pública, pero sin duda lo más importante es que consiguió que la atención de las autoridades y de la ciudadanía se centrara en diversos temas. *WikiLeaks* en definitiva confirma que la aseveración "la información es poder" sigue siendo tan válida hoy cómo en el pasado.

Conclusiones

Las Relaciones Internacionales como objeto de estudio pueden ser abordadas desde distintas perspectivas. Por esta razón diversos teóricos se han dedicado a examinar su estructura, entorno, comportamiento, entre otros factores, en búsqueda de elaborar el retrato más íntegro y apegado a la realidad mundial. Consecuentemente la disciplina de las Relaciones Internacionales ha sido enriquecida con numerosos análisis que a través del tiempo han desafiado, examinado e impulsado viejos y nuevos modelos.

A lo largo de la historia las Relaciones Internacionales han reafirmado su papel como ciencia útil al hombre, puesto que es considerada un elemento esencial en la búsqueda de un sistema interestatal óptimo. Al respecto, en ésta como en cualquier otra disciplina cada proposición es susceptible a ser reexaminada por el paso del tiempo y por la transformación de su entorno y componentes a fin de perfeccionar su estudio.

Ante ello, el presente estudio analizó la forma en que las TIC han impulsado el desarrollo de operaciones de ciberespionaje a nivel internacional; así mismo ha examinado las causas, efectos y circunstancias alrededor del fenómeno *WikiLeaks* y la forma en que modificó la práctica diplomática contemporánea, especialmente la de Canadá.

Para esto, en primera instancia, se ha considerado al espionaje una actividad inherente a la historia del hombre y que con el correr de los años ha comprobado su efectividad como herramienta estratégica durante los conflictos interestatales. En este aspecto se han abordado los cambios experimentados por la Revolución tecnológica donde surge el ciberespionaje como uno de los retos más importantes del siglo XXI para los Estados-nación y el cual ha sido comprobado con la aparición de enormes y sofisticadas operaciones de espionaje cibernético provenientes de países como la República Popular China, Rusia y recientemente Estados Unidos (con el programa PRISMA). Estas prácticas han redefinido los conceptos de soberanía, privacidad, control, cooperación y normativización a nivel internacional en el marco de la Era tecnológica.

De la misma forma se estudian los mecanismos de cooperación multilateral en la materia y se identifica la necesidad de reestablecer nociones como la confianza mutua y el respeto a las

normas internacionales que a lo largo de la historia han constituido el pilar más importante del sistema interestatal.

Bajo este enfoque surgió la necesidad de analizar también los instrumentos jurídicos que a nivel individual han implementado diversas naciones, lo que ha permitido deducir que es después de ataques informáticos o como consecuencia de obligaciones adquiridas en el marco de acuerdos regionales que se han desarrollado mecanismos en contra del ciberespionaje, sin que haya existido un interés genuino al respecto. Sin embargo, es preciso señalar que existe una importante tendencia hacia la optimización de herramientas de seguridad cibernética especialmente de los mecanismos encargados de proteger infraestructura crítica. Dichos esfuerzos se han materializado en Centros de Respuesta a Ataques Cibernéticos que además de extenderse por gran parte del globo han impulsado la cooperación entre determinadas naciones. En este sentido fue imposible examinar forma íntegra las estrategias implementadas por diversas entidades nacionales, regionales y multilaterales debido a la gran cantidad de información que en suma se encuentra constantemente en proceso de actualización. También queda pendiente analizar las formas en las que se investiga un ataque informático dado que las repercusiones internacionales que puede tener una acusación de esta naturaleza son capaces de poner en riesgo la estabilidad mundial, un aspecto nada sencillo y que incluso ha impulsado la creación de una nueva modalidad para los expertos en el ámbito: la informática forense.

Por lo anterior, a la luz de la Teoría de las comunicaciones, se ha examinado la forma en que las nuevas tecnologías han impactado no sólo la relación entre naciones sino los conceptos de seguridad y diplomacia. Gracias a las aportaciones de Tooze, Deutsch, Burton, Nye, Harkiolakis, Arquilla y Ronfeldt, entre otros, se ha deducido una reconfiguración en la dinámica interestatal, la cual se orienta al establecimiento de un complejo sistema de comunicaciones multinivel caracterizado por la incorporación de nuevos participantes y la creación de nuevas vías y rutas de interconexión entre los diversos actores del escenario internacional. Lo cual ha conducido a una transformación en la práctica diplomática tradicional, pues en la actualidad se han incorporado nuevas herramientas y mecanismos con el fin de ejercer eficazmente la práctica diplomática.

Ante este nuevo ecosistema han aparecido nuevas amenazas que desafían tanto la seguridad de las naciones como de la práctica diplomática. Es en este punto donde surge el concepto de

ciberguerra que desde distintas perspectivas se está convirtiendo en elemento dominante dentro múltiples proyecciones sobre enfrentamientos internacionales.

Desde esta óptica la diplomacia moderna se enfrenta a un dilema en el que las TIC aparecen como herramientas capaces de optimizar el ejercicio diplomático convencional, pero también crean nuevas amenazas como el espionaje cibernético y las filtraciones —que en marco del siglo XXI poseen enormes capacidades para dañar a los Estados-nación—. En este sentido se ha determinado una tendencia internacional hacia la macrosecuritización de Internet.

En general se han identificado dos directrices, por un lado quienes afirman que los próximos conflictos interestatales se llevaran a cabo en el ciberespacio, y por otro lado, los que critican dicha suposición al considerar que se tratan de concepciones exageradas y que el armamento cibernético sólo funciona como complemento de las estrategias bélicas convencionales.

Como resultado del análisis de la evolución científico-tecnológica y de su impacto en el sistema internacional, se consideró pertinente examinar también al principal elemento en ellas: el hombre, que bajo la identidad de "Sociedad de la información" juega un papel cada vez más activo en la dinámica mundial. En este sentido el aumento en la injerencia de las ONG, instituciones internacionales y asociaciones civiles propone una redistribución del poder reflejada en nuevos modelos de interacción internacional menos jerárquicos y con mayor número de participantes, en donde se establecen canales de comunicación de doble vía gracias a los cuales la sociedad civil internacional emerge como un actor influyente; no obstante, el Estado conserva supremacía en múltiples cuestiones.

En síntesis es claro que las naciones han adoptado nuevas formas de comunicación y organización al interior de su estructura; nuevos medios de interacción con la ciudadanía, y nuevos canales de comunicación con el resto del mundo, y aunque ello ha provocado la creación de un foro internacional más abierto no se prevé la desaparición del Estado como actor predominante.

Por lo anterior, se ha concluido que la transformación de las comunicaciones afecta la dinámica interestatal de manera cuantitativa —que a su vez es producto de alteraciones cualitativas en los elementos del sistema— generando una reconfiguración.

En otros términos cada vez más actores se incorporan a la dinámica estatal a causa del aumento en sus capacidades de acción (producto de las TIC) y de este modo trasforman la estructura internacional.

En este punto fue imposible examinar —por cuestiones de objetividad y extensión— los otros factores que de acuerdo con Deutsch son necesarios para la subsistencia de cualquier sociedad: adaptabilidad, capacidad de aprendizaje y (en especial) la búsqueda de nuevos objetivos que en el marco de la Era digital representaría un análisis interesante sobre el comportamiento de los Estados-nación.

Abordando el estudio de caso se consideró como punto de partida el fenómeno *WikiLeaks* del cual se analizan antecedentes, surgimiento, estructura, función y consecuencias. Con base a ello, es posible señalar que *WikiLeaks* es una organización sin fines de lucro dedicada a difundir información de interés general sobre casos de corrupción o actividades ilícitas —tanto de estructuras estatales como de organismos privados— que trabaja fundamentalmente gracias a la aportación de *whistleblowers* (informantes) y al trabajo de cientos de voluntarios alrededor del mundo.

Dado que también se examinaron sus principales influencias resultó inevitable incluir las principales características del movimiento *hacker* y la ética que orienta dicha práctica. Desde esta perspectiva la línea bajo la cual se admite el *hacking* es a favor de la sociedad, en otras palabras cuando se ejerce para descubrir casos de abusos o delitos a fin de establecer una especie de vigilancia en pro del bienestar común. Posteriormente se hace énfasis en el impacto de *WikiLeaks* en el ejercicio diplomático tradicional para lo cual se diferencia primero los conceptos de espionaje y filtración, lo que ha llevado a examinar los casos más emblemáticos en los últimos años, conduciendo la investigación a "Los papeles de Pentágono" y al *Watergate* todo esto con el fin de crear un contexto sobre las fugas de información, su importancia en el periodismo de investigación y su papel en la historia política.

Aunado a ello, se establece un panorama sobre la concepción de las TIC entre los miembros de la comunidad internacional para dar paso a un estudio *grosso modo* sobre la reacción de diversos miembros de la escena mundial ante las revelaciones de *WikiLeaks* donde es posible observar diversas tendencias de entre las que destacan dos direcciones: 1) los que apoyaron al

principal afectado (Estados Unidos) como Afganistán, Iraq, Italia, México, entre otros, y 2) los que adoptaron decisiones extremas como Cuba, Ecuador y Venezuela expulsando a representantes estadounidenses de sus respectivos territorios. También se han considerado los retos que plantea dicho evento para la práctica periodística y para el aparato jurídico contemporáneo.

Entre tanto se presta especial atención al uso de las TIC como instrumento a favor de la movilización social, cuyo potencial ha sido evidenciado en las protestas de Túnez y Turquía de las cuales se elabora un breve análisis. Por esta razón se examinan los mecanismos que los Estados adoptarán para hacer frente a la movilización social con base en Internet, y la cual se orienta a una combinación de poder duro y poder blando, en este aspecto también destaca el concepto de ciberdemocracia propuesto por Pierre Levy.

El presente trabajo ha adoptado como objeto de estudio el caso de Canadá y las repercusiones generadas por *WikiLeaks* debido a que fue una de las primeras naciones en impulsar estrategias orientadas al desarrollo y propagación de las TIC y también optó por incorporarlas a las estructuras estatales con el fin de convertirse en líder internacional en el uso de nuevas tecnologías. Por lo cual a través de diversos programas las TIC se convirtieron en un medio de enlace entre la ciudadanía y el gobierno.

En cuanto al impacto de *WikiLeaks* en la política nacional e internacional canadiense a pesar de la de la enorme cantidad de datos —251 187 cables— se lograron determinar los documentos que generaron mayor controversia. A nivel nacional encontramos diversos enfrentamientos entre las facciones políticas canadienses respecto a la postura oficial sobre el cambio climático y también hemos podido identificar un alto grado de participación estadounidense en asuntos internos tanto en cuestión de seguridad nacional como en enfrentamientos con grupos indígenas. Asimismo resulta evidente la presión que dicha nación ejerce en cuestiones de política exterior. En adición, las filtraciones han provocado que diversos comités del Parlamento canadiense discutan diferentes propuestas para mejorar la seguridad cibernética en los ámbitos tanto jurídico como técnico. En cuanto a la política exterior, las publicaciones sin duda alguna dificultarán las negociaciones en torno al Acuerdo Estratégico Trans-Pacífico de Asociación Económica, pues con la publicación del contenido de las negociaciones será difícil que la ciudadanía otorgue apoyo total a dicho instrumento; por otra parte las filtraciones

relacionadas con operaciones de inteligencia canadienses en Medio Oriente indiscutiblemente transformarán la metodología utilizada en dichas prácticas.

Del mismo modo se analizaron las repercusiones del fenómeno *WikiLeaks* para las formas de expresión social en Canadá ─específicamente para el *hacktivismo*─ y en las expectativas de participación social a través de las TIC, para lo cual elaboramos una breve, pero necesaria revisión histórica de los movimientos sociales en Canadá a partir de 1957, y examinamos el surgimiento del movimiento *hacktivista.*

A continuación se elabora una proyección sobre los retos y perspectivas para Canadá en cuestiones como gobierno electrónico, transparencia institucional, participación social a través de las TIC y estructuración de normas para la regulación de la *Word Wide Web*. Para lo cual se examinan una serie de informes que el gobierno canadiense facilita al público en general a través del portal *Statistics Canada.* Adicionalmente, se han buscado otras interpretaciones acudiendo a análisis especializados por parte de entidades académicas, asociaciones civiles y ONG en búsqueda de una óptica neutral. En este sentido, las estrategias para la seguridad de infraestructura crítica y los mecanismos de cooperación multilateral en esta materia merecen ser objeto de futuros estudios.

Como consecuencia se ha identificado que Canadá deberá ampliar el espacio de interacción con la ciudadanía, mejorar los mecanismos de transparencia institucional e implementar nuevas medidas de seguridad cibernética, pues *WikiLeaks* no sólo demostró la debilidad de los mecanismos de seguridad estatal, el impacto en la población reflejó la configuración de una sociedad más activa en el ámbito político e impaciente por formar parte de los procesos de toma de decisiones y estructuración de normas. Especialmente Canadá deberá encontrar un punto de equilibrio entre la diplomacia pública electrónica y la seguridad nacional capaz de: 1) asegurar la accesibilidad a información trascendente a la opinión pública; 2) establecer mecanismos de comunicación interactiva con los representantes oficiales; 3) mantener un proceso de estructuración de política exterior flexible e incluyente, y 4) procurar el buen funcionamiento de la diplomacia contemporánea.

Dada la imposibilidad de abarcar íntegramente las repercusiones de las nuevas tecnologías en la interacción internacional queda pendiente la evaluación de los mecanismos de protección

cibernética hacia infraestructura critica nacional tanto de Canadá como de México. Así mismo es preciso profundizar en el desarrollo de "ejércitos electrónicos" por parte de diversas naciones alrededor del globo y que en los últimos años han sido identificados como culpables de cientos de ataques electrónicos a determinados países.

Después de analizar el impacto de las TIC en la sociedad y en la dinámica internacional se ha obtenido los datos suficientes para sustentar la hipótesis, pues se ha identificado la ausencia de medidas de seguridad (tanto legislativas como técnicas) adecuadas para proteger las comunicaciones oficiales y la infraestructura estatal, lo que ha permitido el aumento de operaciones de espionaje y casos de filtraciones diplomáticas en todo el mundo, y que sumadas a la incesante evolución tecnológica han potencializado tanto los daños como sus alcances. Se ha concluido que el fenómeno *WikiLeaks* se debe en parte a dichas deficiencias pero también a la débil interacción entre las autoridades y la sociedad, sector que en plena Era del conocimiento demanda mayor participación en las dinámicas estatales así como mejores mecanismos de rendición de cuentas y de transparencia institucional. Se ha identificado también que *WikiLeaks* demuestra el potencial de las tecnologías en el siglo XXI y representa a una sociedad cada vez más activa en el ámbito político e internacionalmente más conectada, lo cual evidencia la urgencia de nuevas medidas por parte de los Estados para poner en sincronía la práctica diplomática y las innovaciones tecnológicas.

La *Word Wide Web* se presenta como un nuevo espacio de convivencia social en donde no existen barreras ni soberanía; el surgimiento de ataques desde esta gran autopista virtual demanda la participación de todos los actores del escenario mundial. Sin embargo, en el camino hacia la construcción de un régimen internacional para Internet se encuentran obstáculos como actividades de inteligencia de determinadas naciones que atentan contra la privacidad de los ciudadanos y la soberanía de otros países lo que representa un obstáculo para la cooperación multinivel. Al mismo tiempo, surgen conceptos como los derechos digitales que junto a otros como la trasparencia institucional y la rendición de cuentas constituyen un importante desafío para los Estados-nación.

La presenta investigación va más allá de etiquetar como correcto o incorrecto al fenómeno *WikiLeaks*, desde esta perspectiva es más importante su significado social, internacional y político. Refleja los beneficios y desventajas de la web pero también el surgimiento de una

forma de expresión de una generación que creció y se desarrolló a la par de las TIC. Demuestra que los modelos jerárquicos son obsoletos en la Era del conocimiento y que en la Aldea global el establecimiento de medidas para la regulación de Internet no sólo requerirá de una negociación de corte internacional sino también multinivel donde los Estados, las ONG, organizaciones internacionales y la sociedad tengan la misma oportunidad para intercambiar propuestas.

Una vez más las Relaciones Internacionales demuestran su capacidad de transformarse a un ritmo casi imperceptible, comprobando que lo interesante de esta disciplina —además de ubicarse en su diversidad, alcances y otras peculiaridades— descansa en el carácter dinámico del objeto de estudio que por fortuna constantemente se transforma, reinventa y reconfigura permitiendo conocer nuevos escenarios, capaces de ayudar a comprender aunque sea sólo una parte su naturaleza.

Anexo I Perfil de Julian Assange

Creció en constante movimiento, hijo de padres que se dedicaban al negocio del teatro en Australia.

Ahora, a los 39 años, Julian Assange se encuentra nuevamente en movimiento. Es buscado en Suecia por presuntos delitos sexuales y por funcionarios en todo el mundo por la publicación de miles de documentos conteniendo información confidencial en su página de Internet *WikiLeaks*.

Si ha conseguido construir un escudo de todo tipo alrededor de él, probablemente se deba a que aprendió desde niño a lidiar con la soledad y expuso su mente a la maquinaria que tomaría su vida.

Assange fue descrito por su madre, Christine, como "muy inteligente".

Tenía sólo 16 años cuando le compró una computadora Commodore 64. Era 1987, y no había sitios web. Assange conectó un modem a su computadora y comenzó su viaje a través del creciente mundo de las redes informáticas.

"Es como el ajedrez", le dijo a la revista *New Yorker*. "El ajedrez es muy austero en el hecho de que no tienes muchas reglas, no hay azar y el problema es muy difícil".

Aunque su madre lo educó sin ninguna influencia religiosa, ella sintió que desde una edad temprana, su hijo estaba motivado por un fuerte deseo de hacer lo que percibía como justo.

"Él era un niño adorable, muy sensible, bueno con los animales, tranquilo y con un gran sentido del humor", le dijo este miércoles al periódico *Herald Sun* de Melbourne, Australia.

Él hubiera estudiado matemáticas y física en la Universidad de Melbourne.

En entrevistas, sale a relucir su precisión científica. Habla en una voz de barítono, con un ritmo pausado, escogiendo cuidadosamente cada palabra. Él puede ser encantador aunque cauteloso sobre su vida privada y rara vez es afectado por debates, incluso tras las revelaciones más polémicas en *WikiLeaks*.

Es el tipo de persona que, según se ha descrito, puede introducirse en el sistema computacional más sofisticado. Pero puede olvidar presentarse a una entrevista o cancelarla en el último momento. Cuando habla, el despliega una impresionante amplitud de intereses: desde las computadoras hasta la literatura o sus viajes en África.

Incluso cuando se salió de la entrevista para *CNN* en octubre, después de negarse a responder preguntas sobre las acusaciones sexuales en Suecia, Assange permaneció calmado y sereno. Proyectó un comportamiento señorial, ayudado por su abundancia de cabello gris —que creció a una edad temprana— y una expresión facial igualmente inflexible.

Después de su incursión inicial en las computadoras, Assange incursionó en la encriptación computacional y comenzó a interesarse en la seguridad informática. Alguna vez contó una historia de cómo estableció un rompecabezas de encriptación basado en la manipulación de los números primos.

El artículo del *New Yorker*, publicado a principio de año, describió como en 1991, Assange hackeó la terminal maestra de la empresa de telecomunicaciones Nortel, tras lo que desarrolló un creciente temor a ser arrestado.

Se casó y se convirtió en padre de un niño cuando tenía solamente 18 años, pero la relación se derrumbó y su esposa lo dejó junto con su bebé.

Fue acusado con 31 cargos de hacking en Australia, pero al final sólo pagó una pequeña suma por daños, de acuerdo al *New Yorker*.

El joven hacker comenzó a enfocar su atención lejos de las fallas de la redes a lo que percibía como las malas acciones de los gobiernos.

En un blog publicado en IQ.org en el 2007, escribió:

> *Todo el universo o las estructuras que se perciben es un oponente digno, pero intenta como yo, que no puedo escapar al sonido del sufrimiento. Quizás cuando sea un anciano tendré un gran confort en dar vueltas en un laboratorio y hablar gentilmente a los estudiantes en una tarde de verano, y aceptaré el*

sufrimiento con despreocupación Pero no ahora, hombres en su tope, si tienen la convicción están obligados a actuar en ellas.

Se cree que IQ.org es un blog creado por Assange y está registrado bajo el nombre de "JA", por la misma empresa de dominios de EU que *WikiLeaks*. Tiene la misma dirección postal australiana que la dirección de comunicación con *WikiLeaks*.

Entre una variedad de temas tratados en ese blog, Assange discute matemáticas contra filosofía, la muerte de Kurt Vonnegut, la censura en Irán y la empresa como una Nación-Estado.

Impulsado por sus convicciones como activista y la curiosidad de un periodista, Assange fundó *WikiLeaks* en el 2006. Dormía poco y a veces olvidaba comer. Contrató personal y contó con la ayuda de voluntarios.

Siempre protegió sus fuentes, nunca discute la procedencia de la información.

"La gente debe de entender que *WikiLeaks* ha demostrado ser, sin duda, la fuente de información más confiable que existe, porque publicamos material de fuentes de primera mano y el análisis está basado en esa fuente de primera mano", Assange dijo a *CNN*. "Otras organizaciones, con algunas excepciones, simplemente no son confiables".

El sitio de Internet escaló a la notoriedad en julio, cuando publicó 90,000 documentos secretos sobre la guerra de Afganistán. Fue considerado la mayor fuga de información de inteligencia en la historia de EU.

Después *WikiLeaks* publicó en octubre documentos clasificados de la Guerra de Iraq. Y ahora, esta semana, comenzó a publicar 250,000 cables revelando un tesor [sic] de información diplomática secreta. Algunos elogiaron a *WikiLeaks* como un representante de la libertad de expresión. Pero otros, incluyendo a indignados funcionarios del Pentágono y la Casa Blanca, consideraron irresponsable y quieren callar a *WikiLeaks* por lo que ellos llaman un daño irreparable a la seguridad mundial.

Assange, la elusiva cara pública de *WikiLeaks*, fue catapultado a la fama.

La imagen del delgado, desgarbado, vestido con chamarra de cuero, con piel pálida y una mata de canas salpicó las pantallas de televisión. Todo mundo quería saber cómo lo había logrado el editor en jefe de *WikiLeaks*. La revista *Time* lo nominó como su Persona del Año, llamándolo "un nuevo tipo de denunciante de la era digital".

Pero la notoriedad de Assange no terminó ahí. Poco después de las revelaciones de la guerra afgana, se convirtió en un acusado de un delito sexual en Suecia.

La Corte Penal de Estocolmo giró una orden internacional de arresto para Assange hace dos semanas por causa probable en el caso, diciendo que es sospechoso de violación, abuso sexual y utilización ilegal de la fuerza en dos incidentes separados en agosto. Él podría ser sentenciado a dos años de prisión si es encontrado culpable.

La Interpol giró una alerta máxima por Assange a petición de Suecia.

Assange ha alegado su inocencia y calificó a las acusaciones en Suecia como una campaña de desprestigio. Él también rechazó los informes de luchas internas en *WikiLeaks*.

Fuente: Shubert, Atika; Ashley Frantz y Moni Basu. (Diciembre 3, 2010). "La vida secreta de Julian Assange, el fundador de *WikiLeaks*". Sección: El efecto *WikiLeaks*. *CNN México*. [En línea]. Disponible: <http://mexico.cnn.com/mundo/2010/12/03/la-vida-secreta-de-julian-assange-el-fundador-de-*WikiLeaks*>.
(Consulta 11/ 03/2014).

Anexo II Ciberespionaje y Derecho Internacional: El Convenio sobre ciberdelincuencia de Budapest

El convenio sobre ciberdelincuencia de la Unión Europea es conocido como el instrumento más significativo a nivel internacional para la tipificación, persecución y sanción de delitos informáticos y de operaciones ciberespionaje.

Convenio sobre ciberdelincuencia de Budapest

Budapest, 23.XI.2001

Preámbulo

Los Estados miembros del Consejo de Europa y los demás Estados signatarios del presente Convenio;

Considerando que el objetivo del Consejo de Europa es conseguir una unión más estrecha entre sus miembros;

Reconociendo el interés de intensificar la cooperación con los Estados Partes en el presente Convenio;

Convencidos de la necesidad de aplicar, con carácter prioritario, una política penal común encaminada a proteger a la sociedad frente a la ciberdelincuencia, entre otras formas, mediante la adopción de la legislación adecuada y el fomento de la cooperación internacional;

Conscientes de los profundos cambios provocados por la digitalización, la convergencia y la globalización continua de las redes informáticas;

Preocupados por el riesgo de que las redes informáticas y la información electrónica sean utilizadas igualmente para cometer delitos y de que las pruebas relativas a dichos delitos sean almacenadas y transmitidas por medio de dichas redes;

Reconociendo la necesidad de una cooperación entre los Estados y el sector privado en la lucha contra la ciberdelincuencia, así como la necesidad de proteger los legítimos intereses en la utilización y el desarrollo de las tecnologías de la información;

En la creencia de que la lucha efectiva contra la ciberdelincuencia requiere una cooperación internacional en materia penal reforzada, rápida y operativa;

Convencidos de que el presente Convenio resulta necesario para prevenir los actos dirigidos contra la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, redes y

datos informáticos, así como el abuso de dichos sistemas, redes y datos, mediante la tipificación de esos actos, tal y como se definen en el presente Convenio, y la asunción de poderes suficientes para luchar de forma efectiva contra dichos delitos, facilitando su detección, investigación y sanción, tanto a nivel nacional como internacional, y estableciendo disposiciones que permitan una cooperación internacional rápida y fiable;

Conscientes de la necesidad de garantizar el debido equilibrio entre los intereses de la acción penal y el respeto de los derechos humanos fundamentales consagrados en el Convenio de Consejo de Europa para la Protección de los Derechos Humanos y de las Libertades Fundamentales (1950), el Pacto Internacional de Derechos Civiles y Políticos de las Naciones Unidas (1966) y otros tratados internacionales aplicables en materia de derechos humanos, que reafirman el derecho de todos a defender sus opiniones sin interferencia alguna, así como la libertad de expresión, que comprende la libertad de buscar, obtener y comunicar información e ideas de todo tipo, sin consideración de fronteras, así como el respeto de la intimidad;

Conscientes igualmente del derecho a la protección de los datos personales, tal y como se reconoce, por ejemplo, en el Convenio del Consejo de Europa de 1981 para la protección de las personas con respecto al tratamiento informatizado de datos personales;

Considerando la Convención de las Naciones Unidas sobre los Derechos del Niño (1989) y el Convenio de la Organización Internacional del Trabajo sobre las peores formas de trabajo de los menores (1999);

Teniendo en cuenta los convenios existentes del Consejo de Europa sobre cooperación en materia penal, así como otros tratados similares celebrados entre los Estados miembros del Consejo de Europa y otros Estados, y subrayando que el presente Convenio pretende completar dichos Convenios con objeto de dotar de mayor eficacia las investigaciones y los procedimientos penales relativos a los delitos relacionados con los sistemas y datos informáticos, así como facilitar la obtención de pruebas electrónicas de los delitos;

Congratulándose de las recientes iniciativas encaminadas a mejorar el entendimiento y la cooperación internacional en la lucha contra la ciberdelincuencia, incluidas las medidas adoptadas por las Naciones Unidas, la OCDE, la Unión Europea y el G8;

Recordando las recomendaciones del Comité de Ministros nº R (85) 10 relativa a la aplicación práctica del Convenio europeo de asistencia judicial en materia penal, en relación con las comisiones rogatorias para la vigilancia de las telecomunicaciones, nº R (88) 2 sobre medidas

encaminadas a luchar contra la piratería en materia de propiedad intelectual y derechos afines, nº R (87) 15 relativa a la regulación de la utilización de datos personales por la policía, nº R (95) 4 sobre la protección de los datos personales en el ámbito de los servicios de telecomunicaciones, con especial referencia a los servicios telefónicos, así como nº R (89) 9 sobre la delincuencia relacionada con la informática, que ofrece directrices a los legisladores nacionales para la definición de determinados delitos informáticos, y nº R (95) 13 relativa a las cuestiones de procedimiento penal vinculadas a la tecnología de la información;

Teniendo en cuenta la Resolución nº 1, adoptada por los Ministros europeos de Justicia en su XXI Conferencia (Praga, 10 y 11 de junio de 1997), que recomendaba al Comité de Ministros apoyar las actividades relativas a la ciberdelincuencia desarrolladas por el Comité Europeo de Problemas Penales (CDPC) para aproximar las legislaciones penales nacionales y permitir la utilización de medios de investigación eficaces en materia de delitos informáticos, así como la Resolución nº 3, adoptada en la XXIII Conferencia de Ministros europeos de Justicia (Londres, 8 y 9 de junio de 2000), que animaba a las Partes negociadoras a proseguir sus esfuerzos para encontrar soluciones que permitan que el mayor número posible de Estados pasen a ser Partes en el Convenio, y reconocía la necesidad de un sistema rápido y eficaz de cooperación internacional que refleje debidamente las exigencias específicas de la lucha contra la ciberdelincuencia;

Teniendo asimismo en cuenta el Plan de Acción adoptado por los Jefes de Estado y de Gobierno del Consejo de Europa con ocasión de su Segunda Cumbre (Estrasburgo, 10 y 11 de octubre de 1997), para buscar respuestas comunes ante el desarrollo de las nuevas tecnologías de la información, basadas en las normas y los valores del Consejo de Europa,

Han convenido en lo siguiente:

Capítulo I - Terminología

Artículo 1 - Definiciones

A los efectos del presente Convenio:

a. por "sistema informático" se entenderá todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, siempre que uno o varios de ellos permitan el tratamiento automatizado de datos en ejecución de un programa;
b. por "datos informáticos" se entenderá cualquier representación de hechos, información o conceptos de una forma que permita el tratamiento informático,

incluido un programa diseñado para que un sistema informático ejecute una función;

c. por "proveedor de servicios" se entenderá:
    i. toda entidad pública o privada que ofrezca a los usuarios de sus servicios la posibilidad de comunicar por medio de un sistema informático, y
    ii. cualquier otra entidad que procese o almacene datos informáticos para dicho servicio de comunicación o para los usuarios de ese servicio;
d. por "datos sobre el tráfico" se entenderá cualesquiera datos informáticos relativos a una comunicación por medio de un sistema informático, generados por un sistema informático como elemento de la cadena de comunicación, que indiquen el origen, destino, ruta, hora, fecha, tamaño y duración de la comunicación o el tipo de servicio subyacente.

Capítulo II - Medidas que deberán adoptarse a nivel nacional

Sección 1 - Derecho penal sustantivo

Título 1 - Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos

Artículo 2 - Acceso ilícito

Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno el acceso deliberado e ilegítimo a la totalidad o a una parte de un sistema informático. Cualquier Parte podrá exigir que el delito se cometa infringiendo medidas de seguridad, con la intención de obtener datos informáticos o con otra intención delictiva, o en relación con un sistema informático que esté conectado a otro sistema informático.

Artículo 3 - Interceptación ilícita

Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la interceptación deliberada e ilegítima, por medios técnicos, de datos informáticos comunicados en transmisiones no públicas efectuadas a un sistema informático, desde un sistema informático o dentro del mismo, incluidas las emisiones electromagnéticas procedentes de un sistema informático que contenga dichos datos informáticos. Cualquier Parte podrá exigir que el delito se haya cometido con intención delictiva o en relación con un sistema informático conectado a otro sistema informático.

Artículo 4 - Interferencia en los datos

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la comisión deliberada e ilegítima de actos que dañen, borren, deterioren, alteren o supriman datos informáticos.
2. Cualquier Parte podrá reservarse el derecho a exigir que los actos definidos en el apartado 1 provoquen daños graves.

Artículo 5 - Interferencia en el sistema

Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la obstaculización grave, deliberada e ilegítima del funcionamiento de un sistema informático mediante la introducción, transmisión, provocación de daños, borrado, deterioro, alteración o supresión de datos informáticos.

Artículo 6 - Abuso de los dispositivos

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la comisión deliberada e ilegítima de los siguientes actos:
    a. la producción, venta, obtención para su utilización, importación, difusión u otra forma de puesta a disposición de:
        i. un dispositivo, incluido un programa informático, diseñado o adaptado principalmente para la comisión de cualquiera de los delitos previstos de conformidad con los anteriores artículos 2 a5;
        ii. una contraseña, un código de acceso o datos informáticos similares que permitan tener acceso a la totalidad o a una parte de un sistema informático,

    con el fin de que sean utilizados para la comisión de cualquiera de los delitos contemplados en los artículos 2 a 5; y
    b. la posesión de alguno de los elementos contemplados en los anteriores apartados a.i) o ii) con el fin de que sean utilizados para cometer cualquiera de los delitos previstos en los artículos 2 a 5. Cualquier Parte podrá exigir en su derecho interno que se posea un número determinado de dichos elementos para que se considere que existe responsabilidad penal.

2. No podrá interpretarse que el presente artículo impone responsabilidad penal en los casos en que la producción, venta, obtención para su utilización, importación, difusión u otra forma de puesta a disposición mencionadas en el apartado 1 del presente artículo no tengan por objeto la comisión de un delito previsto de conformidad con los artículos 2 a 5 del presente Convenio, como es el caso de las pruebas autorizadas o de la protección de un sistema informático.
3. Cualquier Parte podrá reservarse el derecho a no aplicar lo dispuesto en el apartado 1 del presente artículo, siempre que la reserva no afecte a la venta, la distribución o cualquier otra puesta a disposición de los elementos indicados en el apartado 1.a.ii) del presente artículo.

Título 2 - Delitos informáticos

Artículo 7 - Falsificación informática

Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno, cuando se cometa de forma deliberada e ilegítima, la introducción, alteración, borrado o supresión de datos informáticos que dé lugar a datos no auténticos, con la intención de que sean tenidos en cuenta o utilizados a efectos legales como si se tratara de datos auténticos, con independencia de que los datos sean o no directamente legibles e inteligibles. Cualquier Parte podrá exigir que exista una intención fraudulenta o una intención delictiva similar para que se considere que existe responsabilidad penal.

Artículo 8 - Fraude informático

Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno los actos deliberados e ilegítimos que causen un perjuicio patrimonial a otra persona mediante:

a. cualquier introducción, alteración, borrado o supresión de datos informáticos;
b. cualquier interferencia en el funcionamiento de un sistema informático, con la intención fraudulenta o delictiva de obtener ilegítimamente un beneficio económico para uno mismo o para otra persona.

Título 3 - Delitos relacionados con el contenido

Artículo 9 - Delitos relacionados con la pornografía infantil

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la comisión deliberada e ilegítima de los siguientes actos:
    a. la producción de pornografía infantil con vistas a su difusión por medio de un sistema informático;
    b. la oferta o la puesta a disposición de pornografía infantil por medio de un sistema informático;
    c. la difusión o transmisión de pornografía infantil por medio de un sistema informático,
    d. la adquisición de pornografía infantil por medio de un sistema informático para uno mismo o para otra persona;
    e. la posesión de pornografía infantil en un sistema informático o en un medio de almacenamiento de datos informáticos.
2. A los efectos del anterior apartado 1, por "pornografía infantil" se entenderá todo material pornográfico que contenga la representación visual de:
    a. un menor comportándose de una forma sexualmente explícita;
    b. una persona que parezca un menor comportándose de una forma sexualmente explícita;
    c. imágenes realistas que representen a un menor comportándose de una forma sexualmente explícita.
3. A los efectos del anterior apartado 2, por "menor" se entenderá toda persona menor de 18 años. No obstante, cualquier Parte podrá establecer un límite de edad inferior, que será como mínimo de 16 años.
4. Cualquier Parte podrá reservarse el derecho a no aplicar, en todo o en parte, las letras d) y e) del apartado 1, y las letras b) y c) del apartado 2.

Título 4 - Delitos relacionados con infracciones de la propiedad intelectual y delos derechos afines

Artículo 10 - Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno las infracciones de la propiedad intelectual, según se definan en la legislación de dicha Parte, de conformidad con las obligaciones

asumidas en aplicación del Acta de París de24 de julio de 1971 por la que se revisó el Convenio de Berna para la protección de las obras literarias y artísticas, del Acuerdo sobre los aspectos delos derechos de propiedad intelectual relacionados con el comercio y del Tratado de la OMPI sobre la propiedad intelectual, a excepción de cualquier derecho moral otorgado por dichos Convenios, cuando esos actos se cometan deliberadamente, a escala comercial y por medio de un sistema informático.

2. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno las infracciones delos derechos afines definidas en la legislación de dicha Parte, de conformidad con las obligaciones que ésta haya asumido en aplicación de la Convención Internacional sobre la protección de los artistas intérpretes o ejecutantes, los productores de fonogramas y los organismos de radiodifusión (Convención de Roma), del Acuerdo sobre los aspectos de los derechos de propiedad intelectual relacionados con el comercio y del Tratado de la OMPI sobre las obras de los intérpretes y ejecutantes y los fonogramas, a excepción de cualquier derecho moral otorgado por dichos Convenios, cuando esos actos se cometan deliberadamente, a escala comercial y por medio de un sistema informático. En circunstancias bien delimitadas, cualquier Parte podrá reservarse el derecho a no exigir responsabilidad penal en virtud de los apartados 1 y 2 del presente artículo, siempre que se disponga de otros recursos efectivos y que dicha reserva no vulnere las obligaciones internacionales que incumban a dicha Parteen aplicación de los instrumentos internacionales mencionados en los apartados1 y 2 del presente artículo.

Título 5 - Otras formas de responsabilidad y de sanciones

Artículo 11 - Tentativa y complicidad

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno cualquier complicidad intencionada con vistas a la comisión de alguno de los delitos previstos de conformidad con los artículos 2 a 10 del presente Convenio, con la intención de que se cometa ese delito.
2. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno cualquier tentativa de comisión de alguno de las delitos previstos de conformidad con los artículos3 a 5, 7, 8, 9.1.a) y c) del presente Convenio, cuando dicha tentativa sea intencionada.

3. Cualquier Estado podrá reservarse el derecho a no aplicar, en todo o en parte, el apartado 2 del presente artículo.

Artículo 12 - Responsabilidad de las personas jurídicas

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para que pueda exigirse responsabilidad a las personas jurídicas por los delitos previstos de conformidad con el presente Convenio, cuando sean cometidos por cuenta de las mismas por cualquier persona física, tanto en calidad individual como en su condición de miembro de un órgano de dicha persona jurídica, que ejerza funciones directivas en la misma, en virtud de:
    a. un poder de representación de la persona jurídica;
    b. una autorización para tomar decisiones en nombre de la persona jurídica;
    c. una autorización para ejercer funciones de control en la persona jurídica.
2. Además de los casos ya previstos en el apartado 1 del presente artículo, cada Parte adoptará las medidas necesarias para asegurar que pueda exigirse responsabilidad a una persona jurídica cuando la falta de vigilancia o de control por parte de una persona física mencionada en el apartado 1 haya hecho posible la comisión de un delito previsto de conformidad con el presente Convenio en beneficio de dicha persona jurídica por una persona física que actúe bajo su autoridad.
3. Con sujeción a los principios jurídicos de cada Parte, la responsabilidad de una persona jurídica podrá ser penal, civil o administrativa.
4. Dicha responsabilidad se entenderá sin perjuicio de la responsabilidad penal delas personas físicas que hayan cometido el delito.

Artículo 13 - Sanciones y medidas

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para que los delitos previstos de conformidad con los artículos 2 a11 puedan dar lugar a la aplicación de sanciones efectivas, proporcionadas y disuasorias, incluidas penas privativas de libertad.
2. Cada Parte garantizará la imposición de sanciones o de medidas penales o no penales efectivas, proporcionadas y disuasorias, incluidas sanciones pecuniarias, a las personas jurídicas consideradas responsables de conformidad con el artículo 12.

Sección 2 - Derecho procesal

Título 1 - Disposiciones comunes

Artículo 14 - Ámbito de aplicación de las disposiciones sobre procedimiento

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para establecer los poderes y procedimientos previstos en la presente Sección para los fines de investigaciones o procedimientos penales específicos.
2. Salvo que se establezca específicamente otra cosa en el artículo 21, cada Parte aplicará los poderes y procedimientos mencionados en el apartado 1 del presente artículo a:
    a. los delitos previstos de conformidad con los artículos 2 a 11 del presente Convenio;
    b. otros delitos cometidos por medio de un sistema informático; y
    c. la obtención de pruebas electrónicas de un delito.
3. a. Cualquier Parte podrá reservarse el derecho a aplicar las medidas indicadas en el artículo 20 exclusivamente a los delitos o categorías de delitos especificados en la reserva, siempre que el ámbito de dichos delitos o categorías de delitos no sea más reducido que el de los delitos a los que esa Parte aplique las medidas indicadas en el artículo 21. Las Partes procurarán limitar dichas reservas para permitir la aplicación más amplia posible de la medida indicada en el artículo 20.
    c. Cuando, como consecuencia de las limitaciones existentes en su legislación vigente en el momento de la adopción del presente Convenio, una Parte no pueda aplicar las medidas indicadas en los artículos 20 y 21 a las comunicaciones transmitidas en el sistema informático de un proveedor de servicios:
        i. utilizado en beneficio de un grupo restringido de usuarios, y
        ii. que no utilice las redes públicas de comunicaciones ni esté conectado a otro sistema informático, ya sea público o privado, dicha Parte podrá reservarse el derecho a no aplicar dichas medidas a esas comunicaciones. Cada Parte procurará limitar este tipo de reservas de forma que se permita la aplicación más amplia posible de las medidas indicadas en los artículos 20 y 21.

Artículo 15 - Condiciones y salvaguardas

1. Cada Parte se asegurará de que el establecimiento, la ejecución y la aplicación de los poderes y procedimientos previstos en la presente sección están sujetas a las condiciones

y salvaguardas previstas en su derecho interno, que deberá garantizar una protección adecuada de los derechos humanos y de las libertades, incluidos los derechos derivados de las obligaciones asumidas en virtud del Convenio del Consejo de Europa para la protección de los derechos humanos y las libertades fundamentales (1950), del Pacto Internacional de derechos civiles y políticos de las Naciones Unidas (1966), y de otros instrumentos internacionales aplicables en materia de derechos humanos, y que deberá integrar el principio de proporcionalidad.

2. Cuando resulte procedente dada la naturaleza del procedimiento o del poder de que se trate, dichas condiciones incluirán, entre otros aspectos, la supervisión judicial u otra forma de supervisión independiente, los motivos que justifiquen la aplicación, y la limitación del ámbito de aplicación y de la duración del poder o del procedimiento de que se trate.
3. Siempre que sea conforme con el interés público y, en particular, con la correcta administración de la justicia, cada Parte examinará la repercusión delos poderes y procedimientos previstos en la presente sección en los derechos, responsabilidades e intereses legítimos de terceros.

Título 2 - Conservación rápida de datos informáticos almacenados

Artículo 16 - Conservación rápida de datos informáticos almacenados

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para permitir a sus autoridades competentes ordenar o imponer de otra manera la conservación rápida de determinados datos electrónicos, incluidos los datos sobre el tráfico, almacenados por medio de un sistema informático, en particular cuando existan razones para creer que los datos informáticos resultan especialmente susceptibles de pérdida o de modificación.
2. Cuando una Parte aplique lo dispuesto en el anterior apartado 1 por medio de una orden impartida a una persona para conservar determinados datos almacenados que se encuentren en posesión o bajo el control de dicha persona, la Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para obligar a esa persona a conservar y a proteger la integridad de dichos datos durante el tiempo necesario, hasta un máximo de noventa días, de manera que las autoridades competentes puedan conseguir su revelación. Las Partes podrán prever que tales órdenes sean renovables.

3. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para obligar al encargado de la custodia de los datos o a otra persona encargada de su conservación a mantener en secreto la aplicación de dichos procedimientos durante el plazo previsto en su derecho interno.
4. Los poderes y procedimientos mencionados en el presente artículo estarán sujetos a lo dispuesto en los artículos 14 y 15.

Artículo 17 - Conservación y revelación parcial rápidas de datos sobre el tráfico

1. Para garantizar la conservación de los datos sobre el tráfico en aplicación de lo dispuesto en el artículo 16, cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias:
    a. para asegurar la posibilidad de conservar rápidamente dichos datos sobre el tráfico con independencia de que en la transmisión de esa comunicación participaran uno o varios proveedores de servicios, y
    b. para garantizar la revelación rápida a la autoridad competente de la Parte, o a una persona designada por dicha autoridad, de un volumen suficiente de datos sobre el tráfico para que dicha Parte pueda identificar a los proveedores de servicio y la vía por la que se transmitió la comunicación.
2. Los poderes y procedimientos mencionados en el presente artículo estarán sujetos a lo dispuesto en los artículos 14 y 15.

Título 3 - Orden de presentación

Artículo 18 - Orden de presentación

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para facultar a sus autoridades competentes a ordenar:
    a. a una persona que se encuentre en su territorio que comunique determinados datos informáticos que posea o que se encuentren bajo su control, almacenados en un sistema informático o en un medio de almacenamiento de datos informáticos; y
    b. a un proveedor de servicios que ofrezca prestaciones en el territorio de esa Parte que comunique los datos que posea o que se encuentren bajo su control relativos a los abonados en conexión con dichos servicios.
2. Los poderes y procedimientos mencionados en el presente artículo están sujetos a lo dispuesto en los artículos 14 y 14.

3. A los efectos del presente artículo, por "datos relativos a los abonados" se entenderá toda información, en forma de datos informáticos o de cualquier otra forma, que posea un proveedor de servicios y esté relacionada con los abonados a dichos servicios, excluidos los datos sobre el tráfico o sobre el contenido, y que permita determinar:
    a. el tipo de servicio de comunicaciones utilizado, las disposiciones técnicas adoptadas al respecto y el periodo de servicio;
    b. la identidad, la dirección postal o geográfica y el número de teléfono del abonado, así como cualquier otro número de acceso o información sobre facturación y pago que se encuentre disponible sobre la base de un contrato o de un acuerdo de prestación de servicios;
    c. cualquier otra información relativa al lugar en que se encuentren los equipos de comunicaciones, disponible sobre la base de un contrato o de un acuerdo de servicios.

Título 4 - Registro y confiscación de datos informáticos almacenados

Artículo 19 - Registro y confiscación de datos informáticos almacenados

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para facultar a sus autoridades competentes a registrar o a tener acceso de una forma similar:
    a. a un sistema informático o a una parte del mismo, así como a los datos informáticos almacenados en el mismo; y
    b. a un medio de almacenamiento de datos informáticos en el que puedan almacenarse datos informáticos, en su territorio.
2. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para asegurar que, cuando sus autoridades procedan al registro o tengan acceso de una forma similar a un sistema informático específico o a una parte del mismo, de conformidad con lo dispuesto en el apartado 1.a, y tengan razones para creer que los datos buscados están almacenados en otro sistema informático o en una parte del mismo situado en su territorio, y dichos datos sean lícitamente accesibles a través del sistema inicial o estén disponibles para éste, dichas autoridades puedan ampliar rápidamente el registro o la forma de acceso similar al otro sistema.
3. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para facultar a sus autoridades competentes a confiscar o a obtener de una forma similar los

datos informáticos a los que se haya tenido acceso en aplicación de lo dispuesto en los apartados 1 ó 2. Estas medidas incluirán las siguientes facultades:

a. confiscar u obtener de una forma similar un sistema informático o una parte del mismo, o un medio de almacenamiento de datos informáticos;
b. realizar y conservar una copia de dichos datos informáticos;
c. preservar la integridad de los datos informáticos almacenados de que se trate;
d. hacer inaccesibles o suprimir dichos datos informáticos del sistema informático al que se ha tenido acceso.

4. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para facultar a sus autoridades competentes a ordenar a cualquier persona que conozca el funcionamiento del sistema informático o las medidas aplicadas para proteger los datos informáticos contenidos en el mismo que facilite toda la información necesaria, dentro de lo razonable, para permitir la aplicación de las medidas indicadas en los apartados 1 y 2.
5. Los poderes y procedimientos mencionados en el presente artículo estarán sujetos a lo dispuesto en los artículos 14 y 15.

Título 5 - Obtención en tiempo real de datos informáticos

Artículo 20 - Obtención en tiempo real de datos sobre el tráfico

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para facultar a sus autoridades competentes a:
    a. obtener o grabar mediante la aplicación de medios técnicos existentes en su territorio, y
    b. obligar a un proveedor de servicios, dentro de los límites de su capacidad técnica:
        i. a obtener o grabar mediante la aplicación de medios técnicos existentes en su territorio, o
        ii. a prestar a las autoridades competentes su colaboración y su asistencia para obtener o grabaren tiempo real los datos sobre el tráfico asociados a comunicaciones específicas transmitidas en su territorio por medio de un sistema informático.
2. Cuando una Parte, en virtud de los principios consagrados en su ordenamiento jurídico interno, no pueda adoptar las medidas indicadas en el apartado 1.a), podrá adoptar en su lugar las medidas legislativas y de otro tipo que resulten necesarias para asegurar la

obtención o la grabación en tiempo real de los datos sobre el tráfico asociados a determinadas comunicaciones transmitidas en su territorio mediante la aplicación de los medios técnicos existentes en el mismo.

3. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para obligar a un proveedor de servicios a mantener en secreto el hecho de que se ha ejercido cualquiera de los poderes previstos en el presente artículo, así como toda información al respecto.
4. Los poderes y procedimientos mencionados en el presente artículo estarán sujetos a lo dispuesto en los artículos 14 y 15.

Artículo 21 - Interceptación de datos sobre el contenido

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para facultar a las autoridades competentes, por lo que respecta a una serie de delitos graves que deberán definirse en su derecho interno:
    a. obtener o a grabar mediante la aplicación de medios técnicos existentes en su territorio, y
    b. a obligar a un proveedor de servicios, dentro de los límites de su capacidad técnica:
        i. a obtener o a grabar mediante la aplicación de los medios técnicos existentes en su territorio, o
        ii. a prestar a las autoridades competentes su colaboración y su asistencia para obtener o grabaren tiempo real los datos sobre el contenido de determinadas comunicaciones en su territorio, transmitidas por medio de un sistema informático.
2. Cuando una Parte, en virtud de los principios consagrados en su ordenamiento jurídico interno, no pueda adoptar las medidas indicadas en el apartado 1.a), podrá adoptar en su lugar las medidas legislativas y de otro tipo que resulten necesarias para asegurar la obtención o la grabación en tiempo real de los datos sobre el contenido de determinadas comunicaciones transmitidas en su territorio mediante la aplicación de los medios técnicos existentes en el mismo.
3. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para obligar a un proveedor de servicios a mantener en secreto el hecho de que se ha ejercido

cualquiera de los poderes previstos en el presente artículo, así como toda información al respecto. Los poderes y procedimientos mencionados en el presente artículo estarán sujetos a lo dispuesto en los artículos 14 y 15.

Sección 3 - Jurisdicción

Artículo 22 – Jurisdicción

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para afirmar su jurisdicción respecto de cualquier delito previsto con arreglo a los artículos 2 a 11 del presente Convenio, siempre que se haya cometido:
    a. en su territorio; o
    b. a bordo de un buque que enarbole pabellón de dicha Parte; o
    c. a bordo de una aeronave matriculada según las leyes de dicha Parte; o
    d. por uno de sus nacionales, si el delito es susceptible de sanción penal en el lugar en el que se cometió o si ningún Estado tiene competencia territorial respecto del mismo.
2. Cualquier Estado podrá reservarse el derecho a no aplicar o a aplicar únicamente en determinados casos o condiciones las normas sobre jurisdicción establecidas en los apartados 1.b) a 1.d) del presente artículo o en cualquier otra parte de los mismos.
3. Cada Parte adoptará las medidas que resulten necesarias para afirmar su jurisdicción respecto de los delitos mencionados en el apartado 1 del artículo 24del presente Convenio, cuando el presunto autor del delito se encuentre en su territorio y no pueda ser extraditado a otra Parte por razón de su nacionalidad, previa solicitud de extradición.
4. El presente Convenio no excluye ninguna jurisdicción penal ejercida por una Parte de conformidad con su derecho interno.
5. Cuando varias Partes reivindiquen su jurisdicción respecto de un presunto delito contemplado en el presente Convenio, las Partes interesadas celebrarán consultas, siempre que sea oportuno, con miras a determinar cuál es la jurisdicción más adecuada para las actuaciones penales.

Capítulo III - Cooperación internacional

Sección 1 - Principios generales

Título 1 - Principios generales relativos a la cooperación internacional

Artículo 23 - Principios generales relativos a la cooperación internacional

Las Partes cooperarán entre sí en la mayor medida posible, de conformidad con las disposiciones del presente capítulo, en aplicación de los instrumentos internacionales aplicables a la cooperación internacional en materia penal, de acuerdos basados en legislación uniforme o recíproca y de su derecho interno, para los fines de las investigaciones o los procedimientos relativos a los delitos relacionados con sistemas y datos informáticos o para la obtención de pruebas electrónicas de los delitos.

Título 2 - Principios relativos a la extradición

Artículo 24 – Extradición

1. a. El presente artículo se aplicará a la extradición entre las Partes por los delitos establecidos en los artículos 2 a 11 del presente Convenio, siempre que estén castigados en la legislación de las dos Partes implicadas con una pena privativa de libertad de una duración máxima de como mínimo un año, o con una pena más grave.
   b. Cuando deba aplicarse una pena mínima diferente en virtud de una cuerdo basado en legislación uniforme o recíproca o de un tratado de extradición aplicable entre dos o más Partes, incluido el Convenio Europeo de Extradición (STE nº 24), se aplicará la pena mínima establecida en virtud de dicho acuerdo o tratado.
2. Se considerará que los delitos mencionados en el apartado 1 del presente artículo están incluidos entre los delitos que dan lugar a extradición en cualquier tratado de extradición vigente entre las Partes. Las Partes se comprometen a incluir dichos delitos entre los que pueden dar lugar a extradición en cualquier tratado de extradición que puedan celebrar entre sí.
3. Cuando una Parte que condicione la extradición a la existencia de un tratado reciba una solicitud de extradición de otra Parte con la que no haya celebrado ningún tratado de extradición, podrá aplicar el presente Convenio como fundamento jurídico de la extradición respecto de cualquier delito mencionado en el apartado 1 del presente artículo.
4. Las Partes que no condicionen la extradición a la existencia de un tratado reconocerán los delitos mencionados en el apartado 1 del presente artículo como delitos que pueden dar lugar a extradición entre ellas.
5. La extradición estará sujeta a las condiciones establecidas en el derecho interno de la Parte requerida o en los tratados de extradición aplicables, incluidos los motivos por los que la Parte requerida puede denegar la extradición.

6. Cuando se deniegue la extradición por un delito mencionado en el apartado 1del presente artículo únicamente por razón de la nacionalidad de la persona buscada o porque la Parte requerida se considera competente respecto de dicho delito, la Parte requerida deberá someter el asunto, a petición de la Parte requirente, a sus autoridades competentes para los fines de las actuaciones penales pertinentes, e informará a su debido tiempo del resultado final a la Parte requirente. Dichas autoridades tomarán su decisión y efectuarán sus investigaciones y procedimientos de la misma manera que para cualquier otro delito de naturaleza comparable, de conformidad con la legislación de dicha Parte.
7. a. Cada Parte comunicará al Secretario General del Consejo de Europa, en el momento de la firma o del depósito de su instrumento de ratificación, aceptación, aprobación o adhesión, el nombre y la dirección de cada autoridad responsable del envío o de la recepción de solicitudes de extradición o de detención provisional en ausencia de un tratado.

   b. El Secretario General del Consejo de Europa creará y mantendrá actualizado un registro de las autoridades designadas por las Partes. Cada Parte garantizará en todo momento la exactitud de los datos que figuren en el registro.

Título 3 - Principios generales relativos a la asistencia mutua

Artículo 25 - Principios generales relativos a la asistencia mutua

1. Las Partes se concederán asistencia mutua en la mayor medida posible para los fines de las investigaciones o procedimientos relativos a delitos relacionados con sistemas y datos informáticos o para la obtención de pruebas en formato electrónico de un delito.
2. Cada Parte adoptará también las medidas legislativas y de otro tipo que resulten necesarias para cumplir las obligaciones establecidas en los artículos 27a 35.
3. En casos de urgencia, cada Parte podrá transmitir solicitudes de asistencia o comunicaciones relacionadas con las mismas por medios rápidos de comunicación, incluidos el fax y el correo electrónico, en la medida en que dichos medios ofrezcan niveles adecuados de seguridad y autenticación(incluido el cifrado, en caso necesario), con confirmación oficial posterior si la Parte requerida lo exige. La Parte requerida aceptará la solicitud y dará respuesta a la misma por cualquiera de estos medios rápidos de comunicación.

4. Salvo que se establezca específicamente otra cosa en los artículos del presente capítulo, la asistencia mutua estará sujeta a las condiciones previstas en el derecho interno de la Parte requerida o en los tratados de asistencia mutua aplicables, incluidos los motivos por los que la Parte requerida puede denegarla cooperación. La Parte requerida no ejercerá el derecho a denegar la asistencia mutua en relación con los delitos mencionados en los artículos 2 a 11únicamente porque la solicitud se refiere a un delito que considera de naturaleza fiscal.
5. Cuando, de conformidad con las disposiciones del presente capítulo, se permita a la Parte requerida condicionar la asistencia mutua a la existencia de una doble tipificación penal, dicha condición se considerará cumplida cuando la conducta constitutiva del delito respecto del cual se solicita la asistencia constituya un delito en virtud de su derecho interno, con independencia de que dicho derecho incluya o no el delito dentro de la misma categoría de delitos o lo denomine o no con la misma terminología que la Parte requirente,.

Artículo 26 - Información espontánea

1. Dentro de los límites de su derecho interno, y sin petición previa, una Parte podrá comunicar a otra Parte información obtenida en el marco de sus propias investigaciones cuando considere que la revelación de dicha información podría ayudar a la Parte receptora a iniciar o llevar a cabo investigaciones o procedimientos en relación con delitos previstos en el presente Convenio o podría dar lugar a una petición de cooperación de dicha Parte en virtud del presente capítulo.
2. Antes de comunicar dicha información, la Parte que la comunique podrá solicitar que se preserve su confidencialidad o que se utilice con sujeción a determinadas condiciones. Si la Parte receptora no puede atender esa solicitud, informará de ello a la otra Parte, que deberá entonces determinar si a pesar de ello debe facilitarse la información o no. Si la Parte destinataria acepta la información en las condiciones establecidas, quedará vinculada por las mismas.

Titulo 4 - Procedimientos relativos a las solicitudes de asistencia mutua en ausencia de acuerdos internacionales aplicables

Artículo 27 - Procedimientos relativos a las solicitudes de asistencia mutua en ausencia de acuerdos internacionales aplicables

1. Cuando entre las Partes requirente y requerida no se encuentre vigente un tratado de asistencia mutua o un acuerdo basado en legislación uniforme o recíproca, serán de aplicación las disposiciones de los apartados 2 a 10 del presente artículo. Las disposiciones del presente artículo no serán de aplicación cuando exista un tratado, acuerdo o legislación de este tipo, salvo que las Partes interesadas convengan en aplicar en su lugar la totalidad o una parte del resto del presente artículo.
2. a. Cada Parte designará una o varias autoridades centrales encargadas de enviar solicitudes de asistencia mutua y de dar respuesta a las mismas, de su ejecución y de su remisión a las autoridades competentes para su ejecución.

   b. Las autoridades centrales se comunicarán directamente entre sí.

   c. En el momento de la firma o del depósito de su instrumento de ratificación, aceptación, aprobación o adhesión, cada Parte comunicará al Secretario General del Consejo de Europa los nombres y direcciones de las autoridades designadas en cumplimiento del presente apartado.

   d. El Secretario General del Consejo de Europa creará y mantendrá actualizado un registro de las autoridades centrales designadas por las Partes. Cada Parte garantizará en todo momento la exactitud de los datos que figuren en el registro.
3. Las solicitudes de asistencia mutua en virtud del presente artículo se ejecutarán de conformidad con los procedimientos especificados por la Parte requirente, salvo que sean incompatibles con la legislación de la Parte requerida.
4. Además de las condiciones o de los motivos de denegación contemplados en el apartado 4 del artículo 25, la Parte requerida podrá denegar la asistencia si:
   a. la solicitud se refiere a un delito que la Parte requerida considera delito político o delito vinculado a un delito político;
   b. la Parte requerida considera que la ejecución de la solicitud podría atentar contra su soberanía, seguridad, orden público u otros intereses esenciales.
5. La Parte requerida podrá posponer su actuación en respuesta a una solicitud cuando dicha actuación pudiera causar perjuicios a investigaciones o procedimientos llevados a cabo por sus autoridades.

6. Antes de denegar o posponer la asistencia, la Parte requerida estudiará, previa consulta cuando proceda con la Parte requirente, si puede atenderse la solicitud parcialmente o con sujeción a las condiciones que considere necesarias.
7. La Parte requerida informará sin demora a la Parte requirente del resultado dela ejecución de una solicitud de asistencia. Deberá motivarse cualquier denegación o aplazamiento de la asistencia solicitada. La Parte requerida informará también a la Parte requirente de cualquier motivo que haga imposible la ejecución de la solicitud o que pueda retrasarla de forma significativa.
8. La Parte requirente podrá solicitar a la Parte requerida que preserve la confidencialidad de la presentación de una solicitud en virtud del presente capítulo y del objeto de la misma, salvo en la medida necesaria para su ejecución. Si la Parte requerida no puede cumplir esta petición de confidencialidad, lo comunicará inmediatamente a la Parte requirente, que determinará entonces si pese a ello debe procederse a la ejecución de la solicitud.
9. a. En casos de urgencia, las solicitudes de asistencia mutua o las comunicaciones al respecto podrán ser enviadas directamente por las autoridades judiciales de la Parte requirente a las autoridades correspondientes de la Parte requerida. En tal caso, se enviará al mismo tiempo copia a la autoridad central de la Parte requerida a través de la autoridad central de la Parte requirente.

   b. Cualquier solicitud o comunicación en virtud de este apartado podrá efectuarse a través de la Organización Internacional de Policía Criminal (INTERPOL).

   c. Cuando se presente una solicitud en aplicación de la letra a) del presente artículo y la autoridad no sea competente para tramitarla, remitirá la solicitud a la autoridad nacional competente e informará directamente a la Parte requirente de dicha remisión.

   d. Las solicitudes y comunicaciones efectuadas en virtud del presente apartado que no impliquen medidas coercitivas podrán ser remitidas directamente por las autoridades competentes de la Parte requirente a las autoridades competentes de la Parte requerida.

   e. En el momento de la firma o el depósito de su instrumento de ratificación, aceptación, aprobación o adhesión, cada Parte podrá informar al Secretario General del Consejo de Europa de que, por razones de eficacia, las solicitudes formuladas en virtud del presente apartado deberán dirigirse a su autoridad central.

Artículo 28 - Confidencialidad y restricción de la utilización

1. En ausencia de un tratado de asistencia mutua o de un acuerdo basado en legislación uniforme o recíproca que esté vigente entre las Partes requirente y requerida, serán de aplicación las disposiciones del presente artículo. Las disposiciones del presente artículo no serán de aplicación cuando exista un tratado, acuerdo o legislación de este tipo, salvo que las Partes interesadas convengan en aplicar en su lugar la totalidad o una parte del resto del presente artículo.
2. La Parte requerida podrá supeditar la entrega de información o material en respuesta a una solicitud a la condición de que:
    a. se preserve su confidencialidad cuando la solicitud de asistencia judicial mutua no pueda ser atendida en ausencia de esta condición, o
    b. no se utilicen para investigaciones o procedimientos distintos de los indicados en la solicitud.
3. Si la Parte requirente no puede cumplir alguna condición de las mencionadas en el apartado 2, informará de ello sin demora a la otra Parte, que determinará en tal caso si pese a ello debe facilitarse la información. Cuando la Parte requirente acepte la condición, quedará vinculada por ella.
4. Cualquier Parte que facilite información o material con sujeción a una condición con arreglo a lo dispuesto en el apartado 2 podrá requerir a la otra Parte que explique, en relación con dicha condición, el uso dado a dicha información o material.

Sección 2 - Disposiciones especiales

Título 1 - Asistencia mutua en materia de medidas provisionales

Artículo 29 - Conservación rápida de datos informáticos almacenados

1. Una Parte podrá solicitar a otra Parte que ordene o asegure de otra forma la conservación rápida de datos almacenados por medio de un sistema informático que se encuentre en el territorio de esa otra Parte, respecto de los cuales la Parte requirente tenga la intención de presentar una solicitud de asistencia mutua con vistas al registro o al acceso de forma similar, la confiscación o la obtención de forma similar, o la revelación de los datos.
2. En las solicitudes de conservación que se formulen en virtud del apartado 1 se indicará:
    a. la autoridad que solicita dicha conservación;
    b. el delito objeto de investigación o de procedimiento penal y un breve resumen de los hechos relacionados con el mismo;

c. los datos informáticos almacenados que deben conservarse y su relación con el delito;
d. cualquier información disponible que permita identificar a la persona encargada de la custodia de los datos informáticos almacenados o la ubicación del sistema informático;
e. la necesidad de la conservación; y
f. que la Parte tiene la intención de presentar una solicitud de asistencia mutua para el registro o el acceso de forma similar, la confiscación o la obtención de forma similar o la revelación de los datos informáticos almacenados.

3. Tras recibir la solicitud de otra Parte, la Parte requerida tomará las medidas adecuadas para conservar rápidamente los datos especificados de conformidad con su derecho interno. A los efectos de responder a una solicitud, no se requerirá la doble tipificación penal como condición para proceder a la conservación.
4. Cuando una Parte exija la doble tipificación penal como condición para atender una solicitud de asistencia mutua para el registro o el acceso de forma similar, la confiscación o la obtención de forma similar o la revelación de datos almacenados, dicha Parte podrá reservarse, en relación con delitos distintos delos previstos con arreglo a los artículos 2 a 11 del presente Convenio, el derecho a denegar la solicitud de conservación en virtud del presente artículo en los casos en que tenga motivos para creer que la condición de la doble tipificación penal no podrá cumplirse en el momento de la revelación.
5. Asimismo, las solicitudes de conservación únicamente podrán denegarse si:
   a. la solicitud hace referencia a un delito que la Parte requerida considera delito político o delito relacionado con un delito político;
   b. la Parte requerida considera que la ejecución de la solicitud podría atentar contra su soberanía, seguridad, orden público u otros intereses esenciales.
6. Cuando la Parte requerida considere que la conservación por sí sola no bastará para garantizar la futura disponibilidad de los datos o pondrá en peligro la confidencialidad de la investigación de la Parte requirente o causará cualquier otro perjuicio a la misma, informará de ello sin demora a la Parte requirente, la cual decidirá entonces si debe pese a ello procederse a la ejecución de la solicitud.
7. Las medidas de conservación adoptadas en respuesta a la solicitud mencionada en el apartado 1 tendrán una duración mínima de sesenta días, con objeto de permitir a la Parte

requirente presentar una solicitud de registro o de acceso de forma similar, confiscación u obtención de forma similar, o de revelación de los datos. Cuando se reciba dicha solicitud, seguirán conservándose los datos hasta que se adopte una decisión sobre la misma.

Artículo 30 - Revelación rápida de datos conservados sobre el tráfico

1. Cuando, con motivo de la ejecución de una solicitud presentada de conformidad con el artículo 29 para la conservación de datos sobre el tráfico en relación con una comunicación específica, la Parte requerida descubra que un proveedor de servicios de otro Estado participó en la transmisión de la comunicación, la Parte requerida revelará rápidamente a la Parte requirente un volumen suficiente de datos sobre el tráfico para identificar al proveedor de servicios y la vía por la que se transmitió la comunicación.
2. La revelación de datos sobre el tráfico en virtud del apartado 1 únicamente podrá denegarse si:
    a. la solicitud hace referencia a un delito que la Parte requerida considera delito político o delito relacionado con un delito político;
    b. la Parte requerida considera que la ejecución de la solicitud podría atentar contra su soberanía, seguridad, orden público u otros intereses esenciales.

Título 2 - Asistencia mutua en relación con los poderes de investigación

Artículo 31 - Asistencia mutua en relación con el acceso a datos informáticos almacenados

1. Una Parte podrá solicitar a otra Parte que registre o acceda de forma similar, confisque u obtenga de forma similar y revele datos almacenados por medio de un sistema informático situado en el territorio de la Parte requerida, incluidos los datos conservados en aplicación del artículo 29.
2. La Parte requerida dará respuesta a la solicitud aplicando los instrumentos internacionales, acuerdos y legislación mencionados en el artículo 23, así como de conformidad con otras disposiciones aplicables en el presente capítulo.
3. Se dará respuesta lo antes posible a la solicitud cuando:
    a. existan motivos para creer que los datos pertinentes están especialmente expuestos al riesgo de pérdida o modificación; o
    b. los instrumentos, acuerdos o legislación mencionados en el apartado 2prevean la cooperación rápida.

Artículo 32 - **Acceso transfronterizo a datos almacenados, con consentimiento o cuando estén a disposición del público**

Una Parte podrá, sin la autorización de otra Parte:

a. tener acceso a datos informáticos almacenados que se encuentren a disposición del público (fuente abierta), con independencia de la ubicación geográfica de dichos datos; o
b. tener acceso o recibir, a través de un sistema informático situado en su territorio, datos informáticos almacenados situados en otra Parte, si la Parte obtiene el consentimiento lícito y voluntario de la persona legalmente autorizada para revelar los datos a la Parte por medio de ese sistema informático.

Artículo 33 - Asistencia mutua para la obtención en tiempo real de datos sobre el tráfico

1. Las Partes se prestarán asistencia mutua para la obtención en tiempo real de datos sobre el tráfico asociados a comunicaciones específicas en su territorio transmitidas por medio de un sistema informático. Con sujeción a lo dispuesto en el apartado 2, dicha asistencia se regirá por las condiciones y procedimientos establecidos en el derecho interno.
2. Cada Parte prestará dicha asistencia como mínimo respecto de los delitos por los que se podría conseguir la obtención en tiempo real de datos sobre el tráfico en un caso similar en su país.

Artículo 34 - Asistencia mutua relativa a la interceptación de datos sobre el contenido

1. Las Partes se prestarán asistencia mutua para la obtención o grabación en tiempo real de datos sobre el contenido de comunicaciones específicas transmitidas por medio de un sistema informático en la medida en que lo permitan sus tratados y el derecho interno aplicables.

Título 3 - Red 24/7

Artículo 35 - Red 24/7

1. Cada Parte designará un punto de contacto disponible las veinticuatro horas del día, siete días a la semana, con objeto de garantizar la prestación de ayuda inmediata para los fines de las investigaciones o procedimientos relacionados con delitos vinculados a sistemas y datos informáticos, o para la obtención de pruebas electrónicas de un delito. Dicha asistencia incluirá los actos tendentes a facilitar las siguientes medidas o su adopción directa, cuando lo permitan la legislación y la práctica internas:

a. el asesoramiento técnico;
b. la conservación de datos en aplicación de los artículos 29 y 30;
c. la obtención de pruebas, el suministro de información jurídica y la localización de sospechosos.

2. a. El punto de contacto de una Parte estará capacitado para mantener comunicaciones con el punto de contacto de otra Parte con carácter urgente.

   b. Si el punto de contacto designado por una Parte no depende de la autoridad o de las autoridades de dicha Parte responsables de la asistencia mutua internacional o de la extradición, el punto de contacto velará por garantizar la coordinación con dicha autoridad o autoridades con carácter urgente.
3. Cada Parte garantizará la disponibilidad de personal debidamente formado y equipado con objeto de facilitar el funcionamiento de la red.

Capítulo IV - Disposiciones finales

Artículo 36 - Firma y entrada en vigor

1. El presente Convenio estará abierto a la firma de los Estados miembros del Consejo de Europa y de los Estados no miembros que hayan participado en su elaboración.
2. El presente Convenio estará sujeto a ratificación, aceptación o aprobación. Los instrumentos de ratificación, aceptación o aprobación se depositarán en poder del Secretario General del Consejo de Europa.
3. El presente Convenio entrará en vigor el primer día del mes siguiente a la expiración de un plazo de tres meses desde la fecha en que cinco Estados, delos cuales tres como mínimo sean Estados miembros del Consejo de Europa, hayan expresado su consentimiento para quedar vinculados por el Convenio de conformidad con lo dispuesto en los apartados 1 y 2.
4. Respecto de cualquier Estado signatario que exprese más adelante su consentimiento para quedar vinculado por el Convenio, éste entrará en vigor el primer día del mes siguiente a la expiración de un plazo de tres meses desde la fecha en que haya expresado su consentimiento para quedar vinculado por el Convenio de conformidad con lo dispuesto en los apartados 1 y 2.

Artículo 37 - Adhesión al Convenio

1. Tras la entrada en vigor del presente Convenio, el Comité de Ministros del Consejo de Europa, previa consulta con los Estados Contratantes del Convenio y una vez obtenido su consentimiento unánime, podrá invitar a adherirse al presente Convenio a cualquier Estado que no sea miembro del Consejo y que no haya participado en su elaboración. La decisión se adoptará por la mayoría establecida en el artículo 20.d) del Estatuto del Consejo de Europa y con el voto unánime de los representantes con derecho a formar parte del Comité de Ministros.
2. Para todo Estado que se adhiera al Convenio de conformidad con lo dispuesto en el anterior apartado 1, el Convenio entrará en vigor el primer día del mes siguiente a la expiración de un plazo de tres meses desde la fecha del depósito del instrumento de adhesión en poder del Secretario General del Consejo de Europa.

Artículo 38 - Aplicación territorial

1. En el momento de la firma o del depósito de su instrumento de ratificación, aceptación, aprobación o adhesión, cada Estado podrá especificar el territorio o territorios a los que se aplicará el presente Convenio.
2. En cualquier momento posterior, mediante declaración dirigida al Secretario General del Consejo de Europa, cualquier Parte podrá hacer extensiva la aplicación del presente Convenio a cualquier otro territorio especificado en la declaración. Respecto de dicho territorio, el Convenio entrará en vigor el primer día del mes siguiente a la expiración de un plazo de tres meses desde la fecha en que el Secretario General haya recibido la declaración.
3. Toda declaración formulada en virtud de los dos apartados anteriores podrá retirarse, respecto de cualquier territorio especificado en la misma, mediante notificación dirigida al Secretario General del Consejo de Europa. La retirada surtirá efecto el primer día del mes siguiente a la expiración de un plazo de tres meses desde la fecha en que el Secretario General haya recibido dicha notificación.

Artículo 39 - Efectos del Convenio

1. La finalidad del presente Convenio es completar los tratados o acuerdos multilaterales o bilaterales aplicables entre las Partes, incluidas las disposiciones de:

   - el Convenio europeo de extradición, abierto a la firma en París el 13 de diciembre de 1957 (STE nº 24);

- el Convenio europeo de asistencia judicial en materia penal, abierto a la firma en Estrasburgo el 20 de abril de 1959 (STE nº30);

- el Protocolo adicional al Convenio europeo de asistencia judicial en materia penal, abierto a la firma en Estrasburgo el 17 de marzo de 1978 (STE nº 99).

2. Si dos o más Partes han celebrado ya un acuerdo o tratado sobre las materias reguladas en el presente Convenio o han regulado de otra forma sus relaciones al respecto, o si lo hacen en el futuro, tendrán derecho a aplicar, en lugar del presente Convenio, dicho acuerdo o tratado o a regular dichas relaciones en consonancia. No obstante, cuando las Partes regulen sus relaciones respecto delas materias contempladas en el presente Convenio de forma distinta a la establecida en el mismo, deberán hacerlo de una forma que no sea incompatible con los objetivos y principios del Convenio.

3. Nada de lo dispuesto en el presente Convenio afectará a otros derechos, restricciones, obligaciones y responsabilidades de las Partes.

Artículo 40 - Declaraciones

Mediante notificación por escrito dirigida al Secretario General del Consejo de Europa, cualquier Estado podrá declarar, en el momento de la firma o del depósito de su instrumento de ratificación, aceptación, aprobación o adhesión, que se acoge a la facultad de exigir elementos complementarios según lo dispuesto en los artículos 2, 3,6.1.b), 7, 9.3 y 27.9.e).

Artículo 41 - Cláusula federal

1. Los Estados federales podrán reservarse el derecho a asumir las obligaciones derivadas del capítulo II del presente Convenio de forma compatible con los principios fundamentales por los que se rija la relación entre su gobierno central y los estados que lo formen u otras entidades territoriales análogas, siempre que siga estando en condiciones de cooperar de conformidad con el capítulo III.
2. Cuando formule una reserva en aplicación del apartado 1, un Estado federal no podrá aplicar los términos de dicha reserva para excluir o reducir sustancialmente sus obligaciones en relación con las medidas contempladas en el capítulo II. En todo caso, deberá dotarse de una capacidad amplia y efectiva que permita la aplicación de las medidas previstas en dicho capítulo.
3. Por lo que respecta a las disposiciones del presente Convenio cuya aplicación sea competencia de los estados federados o de otras entidades territoriales análogas que

no estén obligados por el sistema constitucional de la federación a la adopción de medidas legislativas, el gobierno federal informará de esas disposiciones a las autoridades competentes de dichos estados, junto con su opinión favorable, alentándoles a adoptar las medidas adecuadas para su aplicación.

Artículo 42 - Reservas

Mediante notificación por escrito dirigida al Secretario General del Consejo de Europa, cualquier Estado podrá declarar, en el momento de la firma o del depósito de su instrumento de ratificación, aceptación, aprobación o adhesión, que se acoge a una o varias de las reservas previstas en el apartado 2 del artículo 4, apartado 3 del artículo6, apartado 4 del artículo 9, apartado 3 del artículo 10, apartado 3 del artículo 11,apartado 3 del artículo 14, apartado 2 del artículo 22, apartado 4 del artículo 29 y apartado 1 del artículo 41. No podrán formularse otras reservas.

Artículo 43 - Situación de las reservas y retirada de las mismas

1. La Parte que haya formulado una reserva de conformidad con el artículo 42podrá retirarla en todo o en parte mediante notificación dirigida al Secretario General del Consejo de Europa. Dicha retirada surtirá efecto en la fecha en que el Secretario General reciba la notificación. Si en la notificación se indica que la retirada de una reserva surtirá efecto en una fecha especificada en la misma y ésta es posterior a la fecha en que el Secretario General reciba la notificación, la retirada surtirá efecto en dicha fecha posterior.
2. La Parte que haya formulado una reserva según lo dispuesto en el artículo 42retirará dicha reserva, en todo o en parte, tan pronto como lo permitan las circunstancias.
3. El Secretario General del Consejo de Europa podrá preguntar periódicamente a las Partes que hayan formulado una o varias reservas según lo dispuesto en el artículo 42 acerca de las perspectivas de que se retire dicha reserva.

Artículo 44 – Enmiendas

1. Cualquier Estado Parte podrá proponer enmiendas al presente Convenio, que serán comunicadas por el Secretario General del Consejo de Europa a los Estados miembros del Consejo de Europa, a los Estados no miembros que hayan participado en la elaboración del presente Convenio así como a cualquier Estado que se haya adherido al presente Convenio o que haya sido invitado a adherirse al mismo de conformidad con lo dispuesto en el artículo 37.

2. Las enmiendas propuestas por una Parte serán comunicadas al Comité Europeo de Problemas Penales (CDPC), que presentará al Comité de Ministros su opinión sobre la enmienda propuesta.
3. El Comité de Ministros examinará la enmienda propuesta y la opinión presentada por el CDPC y, previa consulta con los Estados Partes no miembros en el presente Convenio, podrá adoptar la enmienda.
4. El texto de cualquier enmienda adoptada por el Comité de Ministros de conformidad con el apartado 3 del presente artículo será remitido a las Partes para su aceptación.
5. Cualquier enmienda adoptada de conformidad con el apartado 3 del presente artículo entrará en vigor treinta días después de que las Partes hayan comunicado su aceptación de la misma al Secretario General.

Artículo 45 - Solución de controversias

1. Se mantendrá informado al Comité Europeo de Problemas Penales del Consejo de Europa (CDPC) acerca de la interpretación y aplicación del presente Convenio.
2. En caso de controversia entre las Partes sobre la interpretación o aplicación del presente Convenio, éstas intentarán resolver la controversia mediante negociaciones o por cualquier otro medio pacífico de su elección, incluida la sumisión de la controversia al CDPC, a un tribunal arbitral cuyas decisiones serán vinculantes para las Partes o a la Corte Internacional de Justicia, según acuerden las Partes interesadas.

Artículo 46 - Consultas entre las Partes

1. Las Partes se consultarán periódicamente, según sea necesario, con objeto de facilitar:
   a. la utilización y la aplicación efectivas del presente Convenio, incluida la detección de cualquier problema derivado del mismo, así como los efectos de cualquier declaración o reserva formulada de conformidad con el presente Convenio;
   b. el intercambio de información sobre novedades significativas de carácter jurídico, político o tecnológico relacionadas con la ciberdelincuencia y con la obtención de pruebas en formato electrónico;
   c. el estudio de la conveniencia de ampliar o enmendar el presente
2. Se mantendrá periódicamente informado al Comité Europeo de Problemas Penales (CDPC) acerca del resultado de las consultas mencionadas en el apartado 1.

3. Cuando proceda, el CDPC facilitará las consultas mencionadas en el apartado 1y tomará las medidas necesarias para ayudar a las Partes en sus esfuerzos por ampliar o enmendar el Convenio. Como máximo tres años después de la entrada en vigor del presente Convenio, el Comité Europeo de Problemas Penales (CDPC) llevará a cabo, en cooperación con las Partes, una revisión de todas las disposiciones del Convenio y, en caso necesario, recomendará las enmiendas procedentes.
4. Salvo en los casos en que sean asumidos por el Consejo de Europa, los gastos realizados para aplicar lo dispuesto en el apartado 1 serán sufragados por las Partes en la forma que éstas determinen.
5. Las Partes contarán con la asistencia de la Secretaría del Consejo de Europa para desempeñar sus funciones en aplicación del presente artículo.

Artículo 47 – Denuncia

1. Cualquier Parte podrá denunciar en cualquier momento el presente Convenio mediante notificación dirigida al Secretario General del Consejo de Europa.
2. Dicha denuncia surtirá efecto el primer día del mes siguiente a la expiración de un plazo de tres meses desde la fecha en que el Secretario General haya recibido la notificación.

Artículo 48 - Notificación

El Secretario General del Consejo de Europa notificará a los Estados miembros del Consejo de Europa, a los Estados no miembros que hayan participado en la elaboración del presente Convenio y a cualquier Estado que se haya adherido al mismo o que haya sido invitado a hacerlo:

a. cualquier firma;
b. el depósito de cualquier instrumento de ratificación, aceptación, aprobación o adhesión;
c. cualquier fecha de entrada en vigor del presente Convenio de conformidad con los artículos 36 y 37;
d. cualquier declaración formulada en virtud del artículo 40 o reserva formulada de conformidad con el artículo 42;
e. cualquier otro acto, notificación o comunicación relativo al presente Convenio .En fe de lo cual, los infrascritos, debidamente autorizados a tal fin, firman el presente Convenio.

Hecho en Budapest, el 23 de noviembre de 2001, en francés e inglés, siendo ambos textos igualmente auténticos, en un ejemplar único que se depositará en los archivos del Consejo de Europa. El Secretario General del Consejo de Europa remitirá copias certificadas a cada uno

de los Estados Miembros del Consejo de Europa, a los Estados no miembros que hayan participado en la elaboración del presente Convenio y a cualquier Estado invitado a adherirse al mismo.

LA JEFE DE ÁREA DE LA OFICINA DE INTERPRETACIÓN DE LENGUASCERTIFICA: Que la precedente traducción está fiel y literalmente hecha de un documento en francés e inglés que a tal efecto se me ha exhibido. Madrid, a 9 de enero de dos mil dos

Fuente: Consejo de Europa. (Noviembre 23, 2001). Convenio sobre la Ciberdelincuencia. Sitio de tratados del Ministerio de Asuntos Exteriores y Oficina de Interpretación de Lenguas (España). [En línea]. Disponible en: <http://apw.cancilleria.gov.co/tratados/AdjuntosTratados/3012f_CE-2001%20CIBER.PD>. (Consulta 12/03/2014).

Cable 08OTTAWA136

Redactado: 25 de enero de 2008
Clasificación: Sólo para uso oficial
Origen: Embajada de Ottawa

Sobre la imagen estadounidense en Canadá

Acerca de un programa de televisión transmitido por la *CBC* que proyecta una imagen negativa de los funcionarios estadounidenses. De acuerdo con representantes de Washington en Canadá el programa está lleno de estereotipos sobre el gobierno de EE.UU.

E.O. 12958: N/A

TAGS: PGOV [Internal Governmental Affairs], KPAO [Public Affairs Office], CA [Canada]
SUBJECT: PRIMETIME IMAGES OF US-CANADA BORDER PAINT U.S. IN INCREASINGLY NEGATIVE LIGHT

REF ID: 08OTTAWA136

1. (SBU) Summary: *The Canadian Broadcasting Corporation* (CBC) has long gone to great pains to highlight the distinction between Americans and Canadians in its programming, generally at our expense. However, the level of anti-American melodrama has been given a huge boost in the current television season as a number of programs offer Canadian viewers their fill of nefarious American officials carrying out equally nefarious deeds in Canada while Canadian officials either oppose them or fall trying. CIA rendition flights, schemes to steal Canada's water, "the Guantanamo-Syria express," F-16's flying in for bombing runs in Quebec to eliminate escaped terrorists: in response to the onslaught, one media commentator concluded, somewhat tongue-in-cheek, that "apparently, our immigration department's real enemies aren't terrorists or smugglers -- they're Americans." While this situation hardly constitutes a public diplomacy crisis per se, the degree of comfort with which Canadian broadcast entities, including those financed by Canadian tax dollars, twist current events to feed long-standing negative images of the U.S. -- and the extent to which the Canadian public seems willing to indulge in the feast - is noteworthy as an indication of the kind of insidious negative popular stereotyping we are increasingly up against in Canada. End Summary.

"THE BORDER" -CANADA'S ANSWER TO 24, W/O THAT SUTHERLAND GUY

2. (SBU) When American TV and movie producers want action, the formula involves Middle Eastern terrorists, a ticking nuclear device, and a (somewhat ironically, Canadian) guy named Sutherland. Canadian producers don't need to look so far -- they can find all the action they need right on the U.S.-Canadian border. This piece of real estate, which most Americans associate with snow blowing back and forth across an imaginary line, has for the past three weeks been for

Canadian viewers the site of downed rendition flights, F-16 bombing runs, and terrorist suspects being whisked away to Middle Eastern torture facilities. "The Border," which state-owned *CBC* premiered on January 7, attracted an impressive 710,000 viewers on its first showing -- not exactly Hockey Night in Canada, but equivalent to an American program drawing about eight million U.S. viewers. The show depicts Canadian immigration and customs officers' efforts to secure the U.S.-Canadian border and the litany of moral dilemmas they face in doing so. The *CBC* bills the high-budget program as depicting the "new war" on the border and "the few who fight it." While the "war" is supposed to be against criminals and terrorists trying to cross the border, many of the immigration team's battles end up being with U.S. government officials, often in tandem with the CIA-colluding Canadian Security and Intelligence Service (CSIS).

3. (SBU) The clash between the Americans and Canadians got started early in the season and has continued unabated. In episode one a Syrian terrorist with a belt full of gel-based explosives is removed from a plane in Canada while the Canadian-Syrian man sitting next to him is rendered by the CIA/CSIS team to Syria -- a fairly transparent reference to QCIA/CSIS team to Syria -- a fairly transparent reference to the Maher Arar case. Fortunately for the incarcerated individual, the sympathetic Canadian Immigration and Customs Security official recognizes the mistake and shrewdly causes the government to rescue him from a Syrian jail through organized media pressure. The episode ends with a preview of things to come when one of the Canadian immigration officers notes with disgust, "Homeland Security is sending in some hot shot agent."

4. (SBU) Episode two expands on this theme, featuring the arrival of an arrogant, albeit stunningly attractive female DHS officer, sort of a cross between Salma Hayek and Cruella De Vil. The show portrays the DHS official bossing around her stereotypically more compassionate Canadian colleagues while uttering such classic lines as, "Who do you think provides the muscle to protect your fine ideals?" and "You would have killed him. Let the American justice system do it for you." Her fallback line in most situations is "it's a matter of national security."

5. (SBU) But the one-liners and cross-border stereotypes really take off in episode three, in which an American rendition aircraft with three terrorist suspects on the "Guantanamo to Syria express" crashes in Quebec and the terrorists escape -- however, not before killing a Quebec police officer, whose sympathetic widow appears throughout the show. The DHS officer's answer to everything is American firepower, but in this episode even CSIS gets a chance at redemption as the CSIS officer in charge challenges her. Ms. DHS barks back, "You really want to talk territorial sovereignty, or should we talk about getting the terrorists back?" After being chased through the woods of Quebec by a cross-culturally balanced CSIS-JTF2 team which kills a 15-year-old terrorist in a shootout, the bad guys are finally cornered on the side of a pristine Canadian lake. Then, after a conversation with Washington in which she asks "can you bypass NSA and State?" our DHS official calls in an air-strike on the terrorists without Canadian concurrence. Canadian planes, another official has explained, are "already deployed to Afghanistan, helping our neighbors fight their war on terror." With only seconds to spare before the bombs are dropped on the Quebec site, the planes are called off when the CSIS-JTF team affirms positive control over the terrorists. Finally, in a last-minute allowance for redemption, the CSIS officer informs his DHS colleague that the captured terrorists will not be turned over to the U.S. but will stand trial

for the death of the Quebec police officer. She does get the final word, though, hissing the classic phrase "you people are so nave," before the screen goes blank.

DEA ALSO TAKES SOME HITS

6. (SBU) If that isn't enough, "the Border" is only one of the CBC programs featuring cross-border relations. "Intelligence," which depicts a Canadian intelligence unit collaborating with a local drug lord-turned government informant, is just as stinging in its portrayal of U.S.-Canada law enforcement cooperation. Through its two seasons, the program has followed plot lines including a DEA attempt to frame the Canadian informant for murder, a CIA plot to secretly divert Canadian water to the American southwest, and a rogue DEA team that actually starts selling drugs for a profit. A columnist in conservative Canadian daily newspaper "The National Post" commented, "There's no question that the CSIS heroes on 'Intelligence' consider the Americans our most dangerous enemies."

EVEN THE LITTLE MOSQUE GETS IN TO THE ACT

7. (U) Even "Little Mosque on the Prairie," a popular Canadian sitcom that depicts a Muslim community in a small Saskatchewan town, has joined the trend of featuring U.S.-Canada border relations. This time, however, the State Department is the fall guy. A December 2007 episode portrayed a Muslim economics professor trying to remove his name from the No-Fly-List at a U.S. consulate. The show depicts a rude and eccentric U.S. consular officer stereotypically attempting to find any excuse to avoid being helpful. Another episode depicted how an innocent trip across the border became a jumble of frayed nerves as Grandpa was scurried into secondary by U.S. border officials because his name matched something on the watch list. Qhis [sic] name matched something on the watch list.

GIVE US YOUR WATER; OH WHAT THE HECK WE'LL TAKE YOUR COUNTRY TOO

8. (U) And it appears that the season is just warming up. After CIA renditions, DEA murder plots, DHS missteps, and unhelpful consular officers, a U.S. takeover of Canada may have been the only theme left for the *CBC* "H20" mini-series. The series was first broadcast in 2005, when it featured an investigation into an American assassination of the Canadian prime minister and a very broad-based (and wildly implausible) U.S. scheme to steal Canadian water. A two-part sequel, set to be broadcast in March and April 2008, will portray the United States as manipulating innocent, trusting Canadians into voting in favor of Canada's becoming part of the United States. Then, after the United States completely takes over Canada, one brave Canadian unites Canadians and Europeans in an attempt to end America's hegemony. Another program could prove more benign but will certainly include its share of digs against all things American: Global TV reportedly is gearing up for a March 2008 debut of its own border security drama, set to feature Canadian search-and-rescue officers patrolling the U.S.-Canada border.

COMMENT

9. (SBU) EKOS pollster Frank Graves told Poloff he thought that at this point such shows are reflective and not causal in determining attitudes in Canada. They play on the deep-seated caution most Canadians feel toward their large neighbor to the south, a sort of zeitgeist that has been in

the background for decades. As one example, a December 2007 Strategic Counsel poll showed that nine percent of Canadians thought U.S. foreign policy was the greatest threat to the world -- twice as high as those who were concerned about weapons of mass destruction. What Graves does find disturbing -- and here he believes that the causal or reflective question is not important -- is that support for a less porous border is increasing in both Canada and the U.S.: in the U.S. because of generalized fear of terrorism and in Canada because of concern over guns, sovereignty, and the impact that a terrorist attack on the U.S. would have on trade. Graves has detected an increasingly wary attitude over the border that he believes could lead to greater distance between the two countries.

10. (SBU) While there is no single answer to this trend, it does serve to demonstrate the importance of constant creative, and adequately-funded public-diplomacy engagement with Canadians, at all levels and in virtually all parts of the country. We need to do everything we can to make it more difficult for Canadians to fall into the trap of seeing all U.S. policies as the result of nefarious faceless U.S. bureaucrats anxious to squeeze their northern neighbor. While there are those who may rate the need for USG public-diplomacy programs as less vital in Canada than in other nations because our societies are so much alike, we clearly have real challenges here that simply must be adequately addressed.

Visit Canada's Economy and Environment Forum at
http://www.intelink.gov/communities/state/canada

WILKINS

Cable 09OTTAWA218

Redactado: 17 de marzo de 2009
Clasificación: Secreto
Origen: Embajada de Ottawa

Sobre la participación canadiense en Afganistán.

El costo político que Stephen Harper tendría que pagar por la extensión de la misión canadiense en Kandahar, y la presión que el gobierno estadounidense ejerció para que Canadá fijara una postura a más tardar en otoño de 2010.

E.O. 12958: DECL: 03/17/2019
TAGS: PREL MOPS NATO AF CA
SUBJECT: (S) CANADA: RE-CONSIDERING ALL OPTIONS FOR ITS FUTURE MILITARY ROLE IN KANDAHAR?

REF ID: 09OTTAWA218

Classified By: PolMinCouns Scott Bellard, reasons 1.4 (b) and (d)

1. (S/NF) Summary: The minority government of Prime Minister Harper may not have actually ruled out extending Canada's 2,800-member military contingent, including combat forces, in Kandahar beyond 2011. If this government remains in office throughout 2010, operational requirements would force a truly final decision no later than fall 2010, but a further extension of combat forces would be a highly sensitive political football. PM Harper may be banking on President Obama's popularity here and hoping that the results of the USG's policy review on Afghanistan, new international efforts stemming from the March 31 conference on Afghanistan in the Netherlands, and the outcome of the NATO 60th anniversary summit will change Canadian domestic dynamics enough to give this government -- or even its successor -- enough new political flexibility to continue a combat role in addition to whatever reconstruction and development roles Canada will maintain after 2011. End summary.

2. (S/NF) At a March Cabinet 10 meeting, ministers of Prime Minister Stephen Harper's minority government apparently agreed that "all options are back on the table" with respect to Canada's military role in Afghanistan after 2011, according to Department of Foreign Affairs and International Trade (DFAIT) Afghanistan Task Force (FTAG) Senior Advisor David Fairchild (strictly protect). It will take time for the government's public rhetoric to catch up to this "new reality," however, requiring some "patience" on the part of allies, Fairchild commented privately to polmiloff on March
16. He urged that, for now, allies should not publicly press Canada to extend its troop deployment in Kandahar beyond 2011.

3. (S/NF) Fairchild (who will soon complete a three-year assignment in FTAG) added that his "best guess at this point" is that by 2011 Canada's Task Force Kandahar (TFK) will no longer exist. He predicted instead that TFK and its 2,800 member Canadian Forces (CF) contingent under ISAF likely will be subsumed into the fast growing U.S. command structure in RC-S. Fairchild further speculated that Canada might withdraw the CF battle group in 2011 for the one year "operational pause" that Chief of Land Forces General Leslie had envisioned in recent testimony to Parliament (reftel), while leaving about 1,800 to 2,000 troops in place to conduct the kinds of training, mentoring, enabling, and PRT force protection missions that the CF are doing at this time.

4. (C/NF) Operational requirements for any extension would force the government's hand no later than fall 2010, Fairchild noted. If Canada begins to withdraw its troops starting in July 2011, as currently mandated by a March 2008 House of Commons bipartisan motion, the U.S. and other ISAF partners will need at least six months to send replacements into RC-S (January-June 2011) in advance of a subsequent six month long withdrawal or draw-down of CF (July-December 2011), he explained. Canadian and U.S. military and civilian planners will need to have a plan in place by January 1, 2011, he reasoned, in order to ensure that the necessary personnel and infrastructure are in Kandahar throughout that year.

5. (S/NF) Comment: After being explicit publicly and privately that the CF combat mission in Afghanistan would definitely end in 2011 according to the terms of the March 2008 motion, PM Harper and his Cabinet would be venturing into politically sensitive territory to try to re-sell a

further extension to an increasingly dubious Canadian public. Official Opposition Liberal leader Michael Ignatieff -- who has also been firm about the 2011 deadline -- has repeatedly accused PM Harper of going back on his word or obfuscating on other issues (notably, the economic downturns and the government deficit), and a reversal of course on Afghanistan by this government would be a political goldmine for the Liberals. Given the Conservatives' minority status in the House of Commons, the likelihood is high for elections sometime over the next year (with fall 2009 a real possibility). Bad news from Kandahar and repeated deaths of Canadian troops contribute to a growing public perception that Canada has already done more than its share; there is very little public appetite for a continued combat role after 2011. PM Harper may be banking on President Obama's popularity here and hoping that the results of the USG's policy review on Afghanistan, new international efforts stemming from the March 31 conference on Afghanistan in the Netherlands, and the outcomes of the NATO 60th anniversary summit could change Canadian domestic dynamics enough to give this government -- or its successor -- enough political flexibility to enable it to continue a combat role in Afghanistan in addition to whatever reconstruction and development role Canada will maintain after 2011.

Visit Canada's North American partnership community at
http://www.intelink.gov/communities/state/nap /

BREESE

Cable 10MONTREAL1_a

Redactado: 7 de enero de 2010
Clasificación: Confidencial
Origen: Montreal, Canadá

Sobre la Conferencia de Copenhague y la influencia de *Power Corporation* en Jean Charest

Según el cable el ex Primer Ministro de Quebec Jean Charest ha cambiado su posición respecto al cambio climático debido a la influencia que ejerce sobre él Paul Desmarais (director de *Power Corporation*). La corporación interesada en la explotación de las arenas bituminosas de Alberta posee una enorme influencia tanto nivel provincial como federal.

E.O. 12958: DECL: DECLASSIFY UPON ARRIVAL
TAGS: ENRG, CA, PREL, PGOV
SUBJECT: COPENHAGEN CONFERENCE REVEALS QUEBEC OIL SANDS INTERESTS
DERIVED FROM: DSCG 05-1 (B), (D)

REF ID: 10MONTREAL1_a

1. (U/NF) Summary. Controversy over Quebec's aggressive position at the Copenhagen environmental conference shed some surprising light into the connections of powerful provincial interests in the Alberta oil sands. Montreal's two major newspaper chains battled back and forth over Quebec-based *Power Corporation's* (Power Corp) financial ties and the corporation's alleged impact on Premier Charest's actions in Copenhagen. Whether Charest was influenced by

Power Corp to tone down his criticism of the federal government is unclear, but the corporation's provincial and federal influence is undeniable. End Summary.

Charest's Strategy Under Scrutiny

2. (U/NF) Arriving at the COP15 Conference in Copenhagen, Quebec Premier Jean Charest, a strong federalist, openly and actively pushed Canada to do more to reduce its greenhouse gas emissions and signed a pact with 20 sub-national representatives who were similarly unsatisfied with their national governments' positions. Charest's public lobbying of his own federal government sparked strong reaction across Canada, sometimes very critical of Quebec for "undermining" federal environmental policy. Quebec won the *Globe and Mail's* "Denigrate Your Own Country Award", along with Ontario, for its performance in Copenhagen. The controversy continues to simmer in the Montreal news this week.

3. (U/NF) In Quebec, most observers praised what they saw as progressive, green policy by Charest. But Montreal's influential *La Presse* excoriated Charest's "arrogant" strategy, branding him "irresponsible" and disloyal to Ottawa. On December 17th, the paper defended Prime Minister Harper's Copenhagen position, insisting that the oil sands industry was vital for the economy of Canada and Quebec. *La Presse's* stance raised eyebrows in Quebec; the paper is federalist, but rarely so quick to jump to the federal government's defense due to an alleged slight from Quebec. Further, the paper's commentary is usually pro-environment.

4. (U/NF) Top circulation tabloid Journal de Montreal led several commentators in charging that *La Presse's* stance had been dictated by its ownership -- *Power Corporation*, a holding company with substantial financial interests in the oil sands. [Comment: The Ambassador met with *Power Corporation* officials on a recent visit to Montreal discussing the general business and political climate in Quebec in the period just before the controversy broke. The diversified management and holding company based in Montreal ($37 billion USD revenue last year) is owned by the powerful Desmarais family. Paul Sr. and his two sons are among the most influential of Canadians and have strong political and family ties - primarily with the federal Liberals in Canada and the French President Sarkozy. End Comment]

Power Corporation and Oil Sands

5. (U/NF) Although *La Presse* defended its impartiality, it was hard to refute *Power Corporation's* fQancial [sic] interests in the oil sands. *Power Corp* is the largest individual shareholder (4.5%) in the French company Total S.A., and wields further influence with Paul Desmarais, Jr. on Total's board of directors. Total S.A. has invested $6 billion USD in Alberta's oil sands to date, and plans to invest $20 billion USD more over the next two decades. It is the fifth largest publicly-traded integrated international oil and gas company in the world, operating in more than 130 countries, with 96,950 employees.

Comment: Charest Tones Down Criticism

5. (U/NF) It's difficult to say whether Charest was reacting to *La Presse*, pressure from the Desmarais family, or another factor entirely, but by the end of the conference he lay low, passing on further media opportunities to criticize Harper. Since then, he has avoided speaking about

Canada's environmental policies, focusing instead on his own plan to reduce automobile emissions in Quebec. The province is the first in Canada to adopt stricter fuel efficiency standards than the federal government. This legislation takes effect Jan. 14, 2010. Meanwhile, the oil sands controversy continues to play itself out in the media here, with the Desmarais angle as a backdrop.

MCCLENNY

Cable 10OTTAWA29

Redactado: 21 de enero de 2010
Clasificación: Confidencial
Origen: Embajada de Ottawa

Sobre el enfoque de Stephen Harper en el Ártico

De acuerdo con el documento Harper ha utilizado "la preocupación por el Norte" como una herramienta política. Durante las dos campañas de Harper se han elaborado diversas promesas para mejorar la protección del Ártico, sin embargo sólo pocas se han cumplido.

E.O. 12958: DECL: 2020/01/20
TAGS: PREL PBTS PGOV SENV CA XQ
SUBJECT: Canada's Conservative Government and its Arctic Focus

REF ID: 10OTTAWA29

CLASSIFIED BY: Eric Benjaminson, Economic Minister-Counselor, State Department, Embassy Ottawa; REASON: 1.4(D)

1. (C/NF) Summary: Since the day after his initial election victory in January 2006, Canadian PM Stephen Harper has continually played up his government's commitment to defending Canada's "North" (the landmass above 60 degrees North latitude represents about 40% of Canada's total territory, but only has about 100,000 people) and has endeavored to make concern for the Arctic a prime feature of the Conservative political brand. The culmination of that effort was the release of the government's "Northern Strategy" in the summer of 2009. Thus far, the government's ardor for the "North" has translated into only a modest array of actions that have an impact on American and other foreign interests: most significantly an extension of the reach of its pollution protection rules in the Arctic, from 100 nautical miles (nm) to 200 nm. To make further progress in its efforts to "enhance Arctic sovereignty," the government likely needs to leverage the stature, policies, and resources of the United States, the one Arctic neighbor whose national interests are most closely aligned with, Canada's. Numerous observers of the Canadian political scene caution, however, that while Arctic sovereignty is tried and tested as an election issue, the promises made are seldom implemented. End summary.

Conservatives make concern for "The North" part of their political brand...and it works

2. (U) Beginning in mid-2004, the then-minority government of Liberal Prime Minister Paul Martin commenced a rhetorical battle with Denmark over a two-decade old claim to uninhabited Hans Island between Greenland and Ellesmere Island, which culminated in July 2005 when the Canadian Defence Minister and several soldiers actually landed on Hans Island and hoisted the maple leaf flag (they also left a bottle of Canadian whisky). Danish-Canadian tensions were reduced to a simmer by a September 2005 joint statement, but the government's Arctic sovereignty statements of 2004 and the Canadian military efforts the following summer set the stage for Conservative Party leader Stephen Harper to make the North an election issue in the campaign that began in December 2005. "The single most important duty of the federal government is to protect and defend our national sovereignty," he declared in stump speeches invoking "...new and disturbing reports [sic] of American nuclear submarines passing though Canadian waters without obtaining the permission of -- or even notifying -- the Canadian government." Candidate Harper's Arctic plan focused on the construction and deployment of three new armed heavy icebreaking ships, an Arctic Ocean sensor system, as well as the eventual construction of a deep water port in Nunavut to guard the Arctic waters. The message seemed to resonate with the electorate; the Conservatives formed the new government in 2006, but failed to win a majority.

3. (U) Once elected, Harper hit the ground running with frosty rhetoric; on January 26, 2006 Harper (who was still only Prime Minister - designate) used his first post-election press conference to respond to the United States Ambassador's restatement the prior day of the longstanding U.S. position on the Northwest passage. Harper firmly declared that "...the Canadian government will defend our sovereignty...and it is the Canadian people we get our mandate from, not the Ambassador of the United States."

4. (C/NF) PM Harper made a focus on the North a prime feature of the Conservative political brand again in the October 2008 general election. In addition, in his government's annual budgets and in public announcements, he has continued to accentuate the focus on the North. For example, in its budgets over the past four years, the government announced a series of significant Arctic expenditures, including: C$750 million for a new Polar-class ice breaker to replace its sole heavy icebreaker, (which is 40 years old and scheduled to be decommissioned in 2017); millions for mapping of the Extended Continental Shelf and mapping of northern natural resources; and, most recently, a C$250 million dollar economic development agency focused on Canada north of the 60th parallel. The culmination of the branding effort was the release of the government's "Northern Strategy" in the summer of 2009. A consolidation of previous Conservative policy pronouncements, the Strategy largely reflects long-standing Canadian Arctic shibboleths (Enhance Arctic Sovereignty; Promote Social and Economic Development; Protect the Environment; Improve Northern Governance and give greater authority to Northerners) to which previous Canadian governments have periodically given voice. The persistent high public profile which this government has accorded "Northern Issues" and the Arctic is, however, unprecedented and reflects the PM's views that "the North has never been more important to our country" - although one could perhaps paraphrase to state "the North has never been more important to our Party." (Comment: The opposition parties have not developed policies on Canada's role in the Arctic beyond generalities, defaulting "ownership" of a robust, rhetorical northern policy to the

Conservatives that dovetails with party's broader priorities of rebuilding the Canadian Forces and enhancing Canada's international role". End Comment).

5. (U) To underscore his government's commitment to the Arctic, the PM has also visited the Arctic every summer since taking office while holding occasional cabinet meetings in the territorial capitals. In the latest example: as the G8 host in 2010, Canada has chosen to convene the G8 Finance Ministers' meeting in Iqaluit on Baffin Island...in February.

6. (C/NF) The government has also taken steps to amend a few key pieces of legislation to enhance its ability to control shipping in the North. In 2009, new authorities came into force that extended Canada's regulations for pollution violations all the way to the 200 nautical mile EEZ limit. A second proposal that would mandate all ships destined for Canada's Arctic waters to report to Canadian authorities has not yet been finalized in regulation. To date, the changes to the shipping rules are the only efforts that have had an impact on American and other foreign interests. The results of Canada's submission of a claim in 2013 for an Extended Continental Shelf under the United Nations Convention on the Law Of the Sea (UNCLOS) will also have an impact on Canada's neighbors. But, at this juncture, for Canada to advance its "sovereignty" interests there is a need to focus on bilateral and multilateral partnerships with its Arctic neighbors.

Canada's Arctic Foreign Policy

7. (U) According to Foreign Minister Cannon, "our foreign policy is a reflection of our domestic policy." To that end, "through the international dimension of our Northern Strategy-our Arctic foreign policy-we will protect our environmental heritage, promote economic and social development, exercise our sovereignty in this vital region and encourage more effective international governance".

Moreover, in March 2009, when FM Cannon unveiled Canada's Arctic Foreign Policy in the Yukon, he declared that his "utmost priority" is to further strengthen Canada's bilateral engagement with Arctic states. He stated that "The United States is our premier partner in the Arctic," that "we have many shared interests and common purposes-in environmental stewardship, search and rescue, safety, security and sustainable resource development," and that he was looking forward to a more enhanced level of cooperation on Arctic issues with the United States. He noted that this would include exploring "ways to pursue a common agenda," starting in 2013, as Canada and subsequently the United States chair the Arctic Council.

He delivered the same speech in April 2009 at the Center for Strategic and International Studies in Washington DC, further adding in his speech that he had discussed opportunities for enhanced cooperation on shared Arctic interests when he had met with Secretary Clinton earlier that day. In November 2009, during a speech in Toronto to the Economic Club of Canada, the Foreign Minister exclaimed that "Canada, with allies like the United States, is well-placed to take a leadership position in the face of the new challenges and opportunities in the Arctic." Interestingly, while taking questions after the speech, FM Cannon refused to be drawn into any discussion of difference with the United States over the Northwest Passage even when pressed, and instead chose to emphasize Arctic cooperation with the U.S.

8. (C/NF) Comment: Canada places great import on its Arctic partnership with the United States and at this juncture the Conservatives in particular see special value in enhancing that partnership. Not only is that partnership materially significant for Canada, which benefits greatly from American resources invested in Arctic science and in defense infrastructure, but also Canada has much to gain from leveraging the stature and standing of the United States. Among the Arctic coastal states (and perhaps among all countries) Canada and the United States typically have the most closely aligned policy interests and generally share a common viewpoint on international law and common objectives in multilateral fora (such as the Arctic Council). From Canada's point of view, if the two countries can find bilateral common-ground on Arctic issues, the chance for Canadian success is much greater than going it alone against the interests of other countries or groups of countries.

9. (C/NF) Comment Continued: Numerous observers of the Canadian political scene caution, however, that while Arctic sovereignty is tried and tested as an election issue, the promises made are seldom implemented (the armed ice-breakers and ocean sensors that candidate Harper promised in the 2006 election have been forgotten; what will be the fate of the three-quarter billion dollar ice-breaker?). That the PM's public stance on the Arctic may not reflect his private, perhaps more pragmatic, priorities, however, was evident in the fact that during several hours together with Ambassador Jacobson on January 7 and 8, which featured long and wide-ranging conversations, the PM did not once mention the Arctic. End Comment.

JACOBSON

Fuente: *WikiLeaks*. (2010). *Secret US Embassy Cables*. [En línea]. Disponible en: <https://*WikiLeaks*.or>. (Consulta 13/03/2014).

Bibliografía

Abacus Data (Octubre 19-21, 2011). "Public Opinion on Occupy Canada/Wall Street Movement" (part. 6). *Corporate and Community Social Responsibility Research Series*. [En línea]. Disponible en: <http://abacusdata.ca/wp-content/uploads/2011/10/Occupy-CanadaOctober-2011-Report.pdf>. (Consulta 20/12/2013).

Accenture. (2007). *Leadership in customer service: Delivering on the promise*. [En línea]. Disponible en: <https://www.accenture.com/Global/Research_and_Insights/By_Industry/Government_and_Public_Service/default.htm>. (Consulta 20/12/2013).

Accenture. (Noviembre 3, 2005). *Leadership in customer service report: New expectations, new experiences*. [En línea]. Disponible en: <https://www.accenture.com/Global/Research_and_Insights/By_Industry/Government_and_Public_Service/default.htm>. (Consulta 23/11/2013).

Acosta, Nelly. (Enero 20, 2010). "'Operación Aurora', el ciberataque más sofisticado de la historia". *El Economista*. [En línea]. Disponible en: <http://eleconomista.com.mx/tecnociencia/2010/01/20/operacion-aurora-ciberataque-mas-sofisticadohistoria>. (Consulta 23/10/13).

Acurio del Pino, Santiago. (2008).*Delitos Informáticos: Generalidades*. [En línea] Disponible en: <http://www.oa.org/juridico/spanish/cyb_ecu_delitos_inform.pdf>. (Consulta 22/03/2013).

Adonon Djogbènou, Fabien. (2009). *Estudios Africanos* (vol. II). UNAM. México. [En línea]. Disponible en: <http://ciid.politicas.unam.mx/estudios_africanosII/EstudiosAfricanosII.pdf>. (Consulta 30/08/13).

AFP, DPA, Reuters, PL y The Independent. (Julio 2, 2013). "John Kerry alega que 'no es inusual' buscar información de otros países". *La Jornada*, p.3.

AFP y PL (Diciembre 2, 1982). "Nicolaides se propone desplazar a Bignone de la Presidencia argentina: Jack Anderson". *El Día*. [En línea]Disponible en: <http://www.unla.edu.ar/greenstone/collect/archived/index/assoc/HASH9c8a/15cc4de6.dir/doc.pdf>. (Consulta 2/02/2013).

Agencia EFE. (Mayo 30, 2005). "Espionaje industrial en Israel a través de troyanos". *ABC.es*, 30 de mayo de 2005. [En línea]. Disponible en: <http://www.abc.es/hemeroteca/historico-30-052005/abc/Ultima/espionaje-industrial-en-israel-a-travesdetroyanos_202820039620.ht>. (Consulta 05/10/13).

Agence France-Presse. (Mayo 15, 2013). "New Yorker unveils open source whistleblower system designed by activist Aaron Schwartz". *The Raw History*. [En línea]. Disponible en: <http://www.rawstory.com/rs/2013/05/15/new-yorker-unveils-open-source-whistleblower-system-designed-by-activist-aaron-schwartz/>. (Consulta 20/06/2013).

Alba, Víctor. *Watergate: historia de un abuso de poder*. Nauta, España, 1974.

Alcaraz, Yetlaneci. (Julio 4, 2013). "Hipocresía europea". *Proceso*, no. 1915, pp. 52-55.

Alonso, Carles (Diciembre, 2011). "La gobernanza de Internet, hacia una regulación compartida", *Quaderns del CAC*, no. 37, vol. XIV, pp. 73-81. [En línea]. Disponible en: <http://www.cac.cat/pfw_files/cma/recerca/quaderns_cac/Q37_Alonso_ES.pdf>. (Consulta 27/04/2013).

Alperovitch, Dmitri. *Revealed: Operation Shady RAT*. McAfee. [En línea]. Disponible en: <http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf>. (Consulta 23/10/13).

Antentas, Josep María y Esther Vivas (Diciembre, 2009). "De Seattle a la crisis global Viento del sur". *Viento Sur*, no. 107, pp. 30-40. [En línea]. Disponible en: <http://www.vientosur.info/articulosabiertos/VS107_AtentasyVivas_DeSeattlealacrisis.pdf>. (Consulta 23/12/2013).

Angus Reid Public Opinion (Diciembre 9, 2010).*Half of Americans Condemn WikiLeaks. Release; Britons and Canadians Split*. Vision Critical. [En línea]. Disponible en: <http://www.angusreidglobal.com/wp-content/uploads/2010/12/2010.12.09_*WikiLeaks*.pdf>. (Consulta 28/12/2013).

AP. (Noviembre 29, 2010). "Reacciones ante destape de *WikiLeaks*". *Perú 21*. [En línea] Disponible en: <http://peru21.pe/noticia/676471/reacciones-ante-destape-*WikiLeaks*>. (Consulta 02/05/2013).

AP. (Julio 13, 2012). "*WikiLeaks* gana round a Visa y MasterCard". El Economista. [En línea]. Disponible en: <http://eleconomista.com.mx/tecnociencia/2012/07/13/*WikiLeaks*-gana-round-visa-mastercard>. (Consulta 11/05/2014).

Arar, Maher (Diciembre 14, 2010). "Enough Hypocrisy: *WikiLeaks* Is Filling a Vacuum". *The Huffington Post*. [En línea]. Disponible en: <http://www.huffingtonpost.com/maher-arar/enough-hypocrisy-wikileak_b_796238.html>. (Consulta 24/01/2013).

Armchair General. (Marzo, 2009). "The Culper Ring". *Arose.squarespace*, vol. IV, no. 1, pp. 26 - 27. [En línea]. Disponible en: <http://arose.squarespace.com/storage/articles/Culper_Ring.pdf>. (Consulta 25/08/13).

Arquilla, John y David F. Ronfeldt. (1997). *In Athena's Camp: Preparing for Conflict in the Information Age*. RAND Corporation, California.

Arquilla, John y David F. Ronfeldt. (1996). *The Advent of Netwar*. RAND Corporation, Estados Unidos.

Arquilla, John y David F. Ronfeldt. Traduce Francisco Muñoz de Bustillo. (2003). *Redes y guerras en red: el futuro del terrorismo, el crimen organizado y el activismo político.* Alianza, Madrid.

Asamblea General de Naciones Unidas. (Enero 22, 2001). *Resolución aprobada por la Asamblea General 55/63. Lucha contra la utilización de la tecnología de la información con fines delictivos.* Organización de Naciones Unidas. [En línea]. Disponible en: <http://www.unodc.org/pdf/c rime/a_res_55/res5563s.pdf>. (Consulta 20/11/13).

Asia-Pacific Economic Cooperation. (Agosto 19-23, 2002). *APEC Cybersecurity strategy.* Telecommunications and Information Working Group. [En línea]. Disponible en: <http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN012298.pdf>. (Consulta 11/11/13).

AVN (Junio 27, 2010). "Policía detiene a casi 600 manifestantes durante Cumbre del G-20". *Sibci.* [En línea]. Disponible en: <http://static1.avn.info.ve/contenido/polic%C3%ADa-detiene-casi-600-manifestantes-durante-cumb re-del-g-20>. (Consulta 23/12/2013).

Ayén Sánchez, Francisco. (2010). "La Segunda Guerra Mundial. Causas, desarrollo y repercusiones" (Sección Temario de oposiciones de Geografía e Historia). *Proyecto Clio 36.* [En línea]. Disponible en: <http://clio.rediris.es/n36/oposicones/tema70.pdf>. (Consulta 22/09/13).

Bagley, Tennent H. (2007). *Spy Wars*. Estados Unidos: Yale University Press.

Barnet, R. (1997). "Subsidiarity, Enabling Government and Local Governance". En Hobson, H.R. y St-Hilaire, F. (Eds.).*Urban governance and finance: a question of who does* what. Montreal: IRPP, pp.62-79.

Barney, Darin. (2003). *Invasions of Publicity: Digital Networks and the Privatization of the Public Sphere*. En Law Commission of Canada (ed.).*New perspectives on the public-private divide* (pp. 94-122). UBC Press, Canadá.

Barrera Orellana, Felipe. *Análisis de la actividad de inteligencia del Estado y su control público jurídico.* (Tesis de Licenciatura), 2009. Universidad de Chile, Facultad de Derecho,

Santiago de Chile. [En línea]. Disponible en: <http://tesis.uchile.cl/bitstream/handle/2250/106894/de-barrera_f.pdf?sequence=3>. (Consulta 30/08/13).

Bartolozzi, Lozano. (1999). "Diplomacia y conflictividad en la sociedad de la información" en Rodríguez, Andrés R. y Sabada Garrera, T. (Eds). *Periodistas ante conflictos*. Pamplona: EUNSA.

Beckett, Charlie y James Ball. (2012). *WikiLeaks: News in the Networked Era*. Reino Unido: Polity Press.

Bendrath, Ralf; Hofmann, Jeanette; Leib, Volker; Mayer, Peter y Michael Zürn. (2007). *Governing the Internet: The Quest for Legitimate and Effective Rules*. En: Hurrelmann, Achim; Leibfried, Stephan; Martens, Kerstin y Peter Mayer (Ed). *Transforming the Golden Age Nation State*. Houndmills, pp. 130-151.

Benjamin Press, Jordan (2011). *NEWS YOU CAN REALLY USE: Thoughts from Ontario journalists about the what and how of teaching news literacy*. (Tesis de Maestría). Queen's University. Ontario. [En línea]. Disponible en: <http://qspace.library.queensu.ca/bitstream/1974/6414/1/Jordan%20Press%20Thesis.pdf>. (Consulta 12/01/2014).

Boix, Leonardo. (Febrero, 2011). "Cuando los secretos se odian". *Proceso*, no. 1788.

Borthwick, Meg (Mayo 4, 2011). "*WikiLeaks* comes to Canada: Federal failure on aboriginal rights". Rabble.ca. [En línea]. Disponible en: <http://rabble.ca/news/2011/05/*WikiLeaks*-co mes-canada-federal-failure-aboriginal-rights>. (Consulta 20/11/2013).

Brauchli, Marcus. (Enero 2004). *The Washington Post*. "Sworn Statements by Abu Ghraib Detainees". [En línea] Disponible en: <http://www.washingtonpost.com/wpsrv/world/iraq/abughraib/swornstatements042104.html>. (Consulta 19/04/2013).

Bravo A., Mauricio. (2013). *WikiLeaks*: teoría y práctica de un desacato. Santiago de Chile: Ediciones Nueva Fojas Ltda. [En línea]. Disponible en: <http://alainet.org/images/Wikibook.pdf>. (Consulta 11/05/2014).

Bronski, Carl (Mayo 19, 2011). "*WikiLeaks* cable exposes Canadian duplicity in Iraq war". *World Socialist Web Site*. [En línea]. Disponible en: <https://www.wsws.org/en/articles/2011/05/cana-m19.html>. (Consulta 24/01/2014).

Brunvand, Erik (1996). "A Little Bit of Hacker History". *Hacker Folklore Page*. [En línea]. Disponible en: <http://www.cs.utah.edu/~elb/folklore/afs-paper/node3.html>. (Consulta 29/03/2013).

Burton, J. W. (1965). *International Relations: A General Theory*. Cambridge University Press, Londres y Nueva York.

Caballero Díez, Juan Andrés. (Noviembre, 2011). "Gaugamela e Hidaspo dos grandes victorias de Alejandro Magno". *Mundo Historia*. [En línea]. Disponible en: <http://www.mundohistoria.org/blog/articulos_web/labatallahidaspo-326-ac-la-ultima-batalla-alejandro-magn>. (Consulta 23/08/13).

Cáceres, Sebastián. "El acceso a Internet en los países subdesarrollados". *Observatorio de la Sociedad de la Información*, Fundación auna. [En línea]. Disponible en: <http://fundacionange.es/areas/28_observatorio/pdfs/subdesarrollados.pdf>. (Consulta 28/08/2013).

Calduch Cevera. (1993). Rafael. *Dinámica de la Sociedad Internacional*. Madrid: CEURA.

Calvo Roy, José Manuel (Junio 1, 2005). "El 'número dos' del FBI en tiempos de Nixon era Garganta Profunda" *El País*. [En línea]. Disponible en: <http://elpais.com/diario/2005/06/01/internacional/1117576816_850215.html>. (Consulta 14/04/2013).

Caminos Marcet, José María. *Periodismo de investigación: teoría y práctica*. Síntesis, Madrid, 1997.

Campen, Alan D. (1992). *The First Information War: The Story of Communications, Computers, and Intelligence Systems in the Persian Gulf War*. Fairfax: AFCEA International Press.

Canada wiki. (Septiembre 25, 2013). *Reddit*. [En línea]. Disponible en: <http://www.reddit.com/r/canada/wiki/relatedsubreddits>. (Consulta 20/12/2013).

Canadian Security Intelligence Service (1999). "Cyber-terrorism". [En línea]. Disponible en: <http://www.csis-scrs.gc.ca/eng/operat/io2e.html>. (Consulta 27/12/2013).

Carcelén Reluz, Carlos Guillermo. (2009). "Espionaje, guerra y competencia mercantil en el siglo XVII". *Investigaciones Sociales*, vol.13, no. 22, pp.101-116. [En línea]. Disponible en: <http://sisbib.unmsm.edu.pe/bibvirtualdata/publicaciones/inv_sociales/N22_2009/pdf/a06.pdf>. (Consulta 26/08/13).

Carter, Matt (Diciembre 1, 2010). "10 things you don't know about *WikiLeaks* mystery man Julian Assange". *The Toronto Star*. [En línea]. Disponible en: <http://www.thestar.com/news/world/2010/12/01/10_things_you_dont_know_about_*WikiLeaks*_mystery_man_julian_assange.html>. (Consulta 26/01/2014).

Castells, Manuel. (1997). *La era de la información* (vol. I). Alianza editorial, Madrid.

Castells, Manuel. (2001).*La era de la información*, (vol. II). Siglo XXI, México.

Castells, Manuel. *Lliçó inaugural del programa de doctorat sobre la societat de la informació i el coneixement*. Universitat Oberta de Catalunya. [En línea] Disponible en: <http://www.uoc.edu/web/cat/articles/castells/print.html>. (Consulta 26/06/2013).

Cavoukian, Ann y Tom Mitchinson (Abril, 2011). *Promoting Transparency through the Electronic Dissemination of Information*. Information and Privacy Commissioner/Ontario. [En línea]. Disponible en: <http://www.ipc.on.ca/images/resources/up-protrans.pdf>. (Consulta 28/01/2014).

Centro Superior de Estudios de la Defensa Nacional. (Marzo, 2012). *Los Ámbitos No Terrestres en la Guerra Futura: Espacio*. Monografías del CESEDEN, no. 128. [En línea]. Disponible en: <http://www.defensa.gob.es/ceseden/Galerias/destacados/publicaciones/monografias/ficheros/128_LOS_AMBITOS_NO_TERRESRES_EN_LA_GUERRA_FUTURA_ESPACIO.PDF>. (Consulta 03/02/2014).

Ciulla Kamarck, Elaine y Joseph S. Nye Jr (eds.). *Governance.com. Democracy in the Information Age*. Brookings Institution Press. Washington, 2002.

Clemente, Dominique (2008). *Canada's Rights Revolution*. UCB Press, Canadá.

Cockcroft D., James, Henry Frundt y Dale L. Johnson (Noviembre, 1972). "Las compañías multinacionales y el gobierno de Allende". *Punto Final*, no. 171. [En línea] Disponible en: <http://www.pf-memoriahistorica.org/PDFs/1972/PF_171_doc.pdf>. (Consulta 30/01/2013).

Cole, Erick y Sandy Ring. (2006). *Insider Threat: Protecting the Enterprise from Sabotage, Spying, and Theft*. Canadá: Syngress.

Collins, Bill; Paquet, Gilles; Roy, Jeffrey y Chris Wilson (Mayo 10-11, 2002). E-Governance and Smart Communities: A Social Learning Challenge. En *SSHRC Knowledge Based Economy*. Conferencia llevada a cabo en Memorial University of Newfoundland, St. John's, Newfoundland. [En línea]. Disponible en: <http://www.christopherwilson.ca/papers/Nfld_paper_2002.pdf>. (Consulta 25/01/2014).

Comisión de las Comunidades Europeas. (Marzo 30, 2009). *Proteger Europa de ciberataques e interrupciones a gran escala: aumentar la preparación, seguridad y resistencia*. EUR-LEX. [En línea]. Disponible en: <http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:ES:HTML>. (Consulta 10/11/13).

Consejo de Europa. (Noviembre 23, 2001). *Convenio sobre la Ciberdelicuencia*. Serie de Tratados Europeos, no. 185. [En línea]. Disponible en: <http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Convention%20and%20protocol/ETS_185_spanish.PDF>. (Consulta 11/11/13).

Comisión Económica para América Latina y el Caribe. (Febrero, 2008). *La sociedad de la información en América Latina y el Caribe: Desarrollo de las tecnologías y tecnologías para el desarrollo.*División de Desarrollo Productivo y Empresarial, y Programa Sociedad

de la Información. [En línea]. Disponible en: <http://www.oei.es/tic/cepal.pdf>. (Consulta 10/02/2014).

Comisión Económica para América Latina y el Caribe. (2013). *Lista de indicadores para el eLAC2015*. Naciones Unidas, pp. 17-18. [En línea] Disponible en: <http://www.eclac.cl/publicaciones/xml/2/49212/ListadeindicadoresparaeleLAC2015.pdf>. (Consulta 02/07/2013).

Consejo de Europa. (Noviembre 23, 2001). Convenio sobre la Ciberdelincuencia. Sitio de tratados del Ministerio de Asuntos Exteriores y Oficina de Interpretación de Lenguas (España). [En línea]. Disponible en: <http://apw.cancilleria.gov.co/tratados/AdjuntosTratados/3012f_CE2001%20CIBER.PDF>. (Consulta 12/03/2014).

Consejo Nacional de Política Económica y Social. (Julio 14, 2011). *Lineamientos de Política para Ciberseguridad y Ciberdefensa*. Conpes 3701. Bogotá. [En línea]. Disponible en: <https://www.dnp.gov.co/LinkClick.aspx?fileticket=-lf5n8mSOuM%3D&tabid=1260>. (Consulta 20/11/13).

CSIS Global Organized Crime Project, Center for Strategic and International Studies. (1998). *Cybercrime-- Cyberterrorism-- Cyberwarfare--: Averting an Electronic Waterloo*. Washington, D.C.: CSIS Press.

Cuen, David (Diciembre 10, 2010). "*WikiLeaks*: denuncian censura en las redes sociales".*BBC*. [En línea]. Disponible en: <http://www.bbc.co.uk/mundo/noticias/2010/12/101213_1112_*WikiLeaks*_twitter_redes_sociales_facebook_algoritmo_dc.shtml>. (Consulta 24/05/2013).

De Castro de Ruano, José Luis. (2000). "Medios de comunicación y las Relaciones Internacionales". En *Cursos de Derecho Internacional y Relaciones Internacionales de Vitoria-Casteiz 1999*. Servicio Editorial de la Universidad del País Vasco, Bilbao.

De las Cuevas, Rafael y Sara Puerto. "Ali Bey, el espía que quiso reinar". La Aventura de la Historia. [En línea]. Disponible en: <http://www.elmundo.es/ladh/numero69/alibey.html>. (Consulta 30/08/13).

De los Santos, Sergio. (Enero 17, 2013). "Operación octubre rojo: un malware muy 'personal'". *Hispasec*. [En línea]. Disponible en: <http://unaaldia.hispasec.com/2013/01/operacion-octubre-rojo-un-malware-muy.html>. (Consulta 05/11/13).

Del Arenal, Celestino. (1985). "En Nuevo Orden Mundial de la Información y de la Comunicación". *Revista de Estudios Internacionales*, no. 1.

Deibert, Ron (Diciembre 11, 2010). "The Post-Cablegate Era". *The New York Times*. [En línea]. Disponible en: <http://www.nytimes.com/roomfordebate/2010/12/09/what-has-*WikiLeaks*-started/after-*WikiLeaks*-a-new-era>. (Consulta 23/01/2014).

Democracy Now (Diciembre 12, 2010). "¡Que democracia!: Departamento de Estado prohíbe *WikiLeaks* a personal y amenaza a estudiantes que los citen". *Aporrea*. [En línea] Disponible en: <http://www.aporrea.org/tiburon/n170786.html>. (Consulta 26/04/2013).

Denning, Dorothy E. (2001). "Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy". *Rand Corporation*. [En línea]. Disponible en: <http://www.rand.org/content/dam/rand/pubs/monograph_reports/MR1382/MR1382.ch8.pdf>. (Consulta 20/01/2014).

Dertouzos, Michael. *What Will Be: How the New World of Information Will Change Our Lives*. Harper Collins, San Francisco, 1997.

Descôteaux, Bernard. "NDLR: Extraits des portions du câble diplomatique qui touchent la conférence de Copenhague, la position du Québec et l'influence de la famille Desmarais". Le Devoir [En línea]. Disponible en: <http://www.ledevoir.com/*WikiLeaks*-power>. (Consulta 23/11/2013).

Deutsch, Karl W. (1981). Trad. de Eduardo L. Suárez. *Las Naciones En Crisis*. Fondo de Cultura Económica. México.

Dorling, Philip (Octubre 29, 2011). "Assange can still Occupy centre stage". *The Sindey Morning Herald*. [En línea]. Disponible en: <http://www.smh.com.au/technology/technol ogy-news /assange-can-still-occupy-centre-stage-20111028-1mo8x.html>. (Consulta 21/11/2013).

DTP. "Countdown to the Battle of Seattle". *Do or Die*, no. 9, pp. 129-133. [En línea]. Disponible en: <http://www.eco-action.org/dod/no9/seattle_chronology.html>. (Consulta 23/12/2013).

Dunn, Miriam A. (2007). *Securing the digital age*. En: Eriksson, Johan y Giampiero Giacomello (eds.). *International Relations and Security in the Digital Age*. Routledge, London.

Durón García, Carlos (2013). Columna "Recopilaciones", *La Prensa*. [En línea] Disponible en: <http://www.oem.com.mx/laprensa/notas/n2904963.htm>. (Consulta 24/06/2013).

Ealy Ortiz, Juan Francisco (Junio 3, 2013). "Twitter, una maldición para la sociedad, acusa Turquía". *El Universal*. [En línea]. Disponible en: <http://www.eluniversal.com.mx/notas/927283.html>. (Consulta 13/05/2013).

EFE (Noviembre 26, 2010). "EE.UU. alerta a 6 Gobiernos por la próxima filtración de *WikiLeaks*". *La vanguardia*. [En línea]. Disponible en: <http://www.lavanguardia.com/20

101126/54075422576/ee-uu-alerta-a-6-gobiernos-por-la-proximafiltraciondeWikiLeaks.h>. (Consulta 11/11/2013).

EFE (Noviembre 30, 2010). "*WikiLeaks* dejó al imperio al desnudo, dice el presidente Hugo Chávez". *CNN México*. [En línea] Disponible en: <http://mexico.cnn.com/mundo/2010/11/30/*WikiLeaks*-dejo-al-imperio-al-desnudo-dice-el-presidente-hugo-chavez>. (Consulta 20/06/2013).

Eriksson, Johan y Giampiero Giacomello. *International Relations and Security in the Digital Age*. Routledge. Reino Unido, 2007.

Espino López, Antonio. (Julio-Diciembre, 2012). "Granada, Canarias, América: el uso de prácticas aterrorizantes en la praxis de tres conquistas, 1482-1557". *Historia,* no. 45, vol. II, pp. 369-398. [En línea]. Disponible en: <http://www.scielo.cl/pdf/historia/v45n2/art01.pdf>. (Consulta 11/08/13).

Europa, Síntesis de la Legislación de la UE. (Marzo 22, 2013). *Agencia Europea de Seguridad de las Redes y de la Información (ENISA)*. [En línea]. Disponible en: <http://europa.eu/legislation_summaries/information_society/internet/l24153_es.htm>. (Consulta 11/11/13).

Fraser, Charmaine (2009). "E-Government: The Canadian Experience". *Dalhousie Journal of Interdisciplinary Management*, vol. 4, pp. 1-14. [En línea]. Disponible en: <http://djim.management.dal.ca/issue_pdfs/Vol4/Fraser_The_Canadian_Experience.pdf>. (Consulta 24/01/2014).

Fidler, Roger F. *Mediamorfosi, Granica.* SA-Adelphi, 1998.

Finch, Gavin y Warren Giles (Enero17, 2011). "*WikiLeaks* to Publish Data from Ex-Julius Baer Banker". *Bloomberg L.P.* [En línea]. Disponible en: <http://www.bloomberg.com/news/2011-01-17/*WikiLeaks*-to-publish-client-datafrom-ex-julius-baer-banker.html>. (Consulta 11/01/2014).

Flemingh, Andrew (Septiembre 27, 2011). "Adbusters sparks Wall Street protest". *Vancouver Courier*. [En línea]. Disponible en: <http://www.vancourier.com/news/adbusters-sparks-wall-street-protest-1.374299>. (Consulta 21/11/2013).

Flores Vivar, Jesús. *Ciberperiodismo: nuevos enfoques, conceptos y profesiones emergentes en el mundo infodigital*. Limusa. México, 2010.

Freeze, Colin (Agosto 23, 2012). "Canadian spy secrets exposed in *WikiLeaks* dump". *The Globe and Mail*. [En línea]. Disponible en: <http://m.theglobeandmail.com/news/politics/canadian-spy-secrets-exposed-in-*WikiLeaks*-dump/article1316198/?>. (Consulta 21/01/2014).

Gandhi, Sajit (Diciembre, 2002). *The Tilt: The U.S. and the South Asian Crisis of 1971*. National Security Archive Electronic Briefing Book, no. 79. [En línea]. Disponible en: <http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB79/>. (Consulta 10/02/2013).

Galván Ochoa, Enrique. (Abril 2, 2012). "De la Madrid nos hizo millonarios... por poco tiempo" columna Dinero, *La Jornada*. [En línea] Disponible en: <http://www.jornada.unam.mx/2012/04/02/opinion/008o1eco>. (Consulta 10/02/2013).

García, Sínide y Nahuel Staudacher. (Julio 7, 2008). "Una de las pruebas 'sucias' de la guerra de Irak: Caso Plame". *NanoMundo*. [En línea]. Disponible en: <http://www.nanomundo.com/index.php/comunicacion/nanoobservatorio/172-caso-plame>. (Consulta 30/03/2013).

Garduño Vera, Roberto. (Septiembre 10, 2004). "La Sociedad de la Información en México frente al uso de Internet". *Revista Digital Universitaria*, vol. 5, no. 8, pp. 2-13. [En línea]. Disponible en: <http://www.revista.unam.mx/vol.5/num8/art50/sep_art50.pdf>. (Consulta10/02/2014).

Geist, Michael (Noviembre 19, 2013). *Leaked TPP Text Confirms Countries Had Plenty to hide* [Blog]. Disponible en: <http://www.michaelgeist.ca/content/view/7001/135/>. (Consulta 21/01/2014).

Geist, Michael (Noviembre 15, 2013). *The TPP IP Chapter Leaks: U.S. Demanding Overhaul of Canadian Anti-Counterfeiting Bill* [Blog]. Disponible en: <http://www.michaelgeist.ca/content/view/6997/125/>. (Consulta 21/01/2014).

Geist, Michael (Noviembre 18, 2013). *The TPP IP Chapter Leaks: U.S. Wants New Regulations for Country-Code Domain Names* [Blog]. Disponible en: <http://www.michaelgeist.ca/content/view/7002/125/>. (Consulta 21/01/2014).

Geist, Michael (2008-2013). *WikiLeaks* [Blog]. Disponible en: <http://www.michaelgeist.ca/index.php?option=com_search&Itemid=99999999&searchword=*WikiLeaks*&searchphrase=any&ordering=newest&limit=50&limitstart=0>. (Consulta 23/01/2014).

Genosko, Gary. (2006). "FCJ-057 The Case of 'Mafiaboy' and the Rhetorical Limits of Hacktivism". *The Fibreculture Journal*, no. 9. [En línea]. Disponible en: <http://nine.fibreculturejournal.org/fcj-057/>. (Consulta 27/12/2013).

Glassford, Lieut. W. A. (Octubre 30, 2002). "The Signal Corps". US Army Center of Military History. [En línea]. Disponible en: <http://www.history.army.mil/books/R&H/R&H-SC.htm>. (Consulta 09/05/2014).

Global Organized Crime Project. (1998). *Cybercrime-cyberterrorism-cyberwarfare-: averting an electronic Waterloo*. Washington, D.C.: Center for Strategic and International Studies.

Goldsmith, J. (1998). "Against Cyberanarchy". *University of Chicago Law Review*, vol. 3, 1199-1250.

González, Omar (Octubre 2011). "Cronología: *WikiLeaks* apaga el altavoz de los secretos oficiales". *Excélsior*. [En línea]. Disponible en: <http://www.excelsior.com.mx/2011/10/24/global/776812>. (Consulta 1/04/2013).

Government of Canada (Enero 8, 2013). *Canada's Action Plan on Open Government.*Data.gc.ca. [En línea]. Disponible en: <http://data.gc.ca/eng/canadas-action-plan-open-government#toc2>. (Consulta 26/01/2014).

Greenwald, Gleen y Ewen MacAskill. (Junio 11, 2013). "Boundless Informant: the NSA's secret tool to track global surveillance data". *The Guardian*. [En línea]. Disponible en: <http://www.theguardian.com/world/2013/jun/08/nsa-boundless-informant-globaldatamining#>. (Consulta 05/11/13).

Greenwald, Gleen y Laura Potras. Traducción de Leonardo Boix. (Julio 14, 2013). "Los motivos de Snowden". *Proceso*, no. 1915, pp. 50-55.

Grou, Vincent (Febrero 8, 2011). "*WikiLeaks* inspire QuébecLeaks". *Sur le Web*. [En línea]. Disponible en: <http://blogues.radio-canada.ca/surleweb/2011/02/08/*WikiLeaks*-inspire-qu ebecleaks/>. (Consulta 27/12/2013).

Guichaoua, Valérie y Sophie Radermecker. (2011). *Julian Assange-WikiLeaks, Warrior For Truth*. Cogito Media Group, Estados Unidos.

Guzmán, Jorge. (1993). *Ay mamá Inés: crónica testimonial*. Santiago de Chile: Andres Bello.

Habermas, Jürgen. (2001). "The Public Sphere: An Encyclopedia Article". En: Durham, M.G. y D.M. Kellner (Eds.). *Media and Cultural Studies*. Blackwell, Oxford, pp. 7-102.

Habermas, Jürgen. Traduce T. McCarthy. (1987). *Theory of Communicative Action* (vol. 2). *Lifeworld and System: A Critique of Functionalist Reason*.Beacon Press, Boston.

Hacker, Kenneth y Jon Van Dijk. *Digital Democracy. Issues of Theory and Practice*. SAGE. Reino Unido, 2000.

Hageman, Mark C. "Espionage in the Civil War". *Spies, scouts and raiders*. [En línea]. Disponible en: <http://www.civilwarsignals.org/pages/spy/spy.html>. (Consulta 30/08/13).

Hampson, Noah C.N. (Enero 5, 2012). "Hacktivism: A New Breed of Protest in a Networked World". *Boston College International and Comparative Law Review* (artículo 6), vol. 35, no. 2. [En línea]. Disponible en: <http://law digitalcommons.bc.edu/cgi/viewcontent.cgi?article=1685&context=iclr>. (Consulta 26/12/2013).

Hannah Arendt (1958). *The Human Condition*. University of Chicago Press, Chicago.

Harter, John-Henry (2011). *New Social Movements, Class, and the Environment: A Case Study of Greenpeace Canada*. Cambridge Scholars Publishing. [En línea]. Disponible en: <http://www.c-s-p.org/flyers/978-1-4438-2863-5-sample.pdf>. (Consulta 23/12/2013).

Harkiolakis, Nicholas. (*s.f.*). *The world of e in diplomacy and negotiations*. Institute of Diplomacy and Global Affairs. [En línea]. Disponible en: <http://www.acg.edu/sites/default/files/pdfs/E-diplomacy.pdf>. (Consulta 10/02/2014).

Harkiolakis, Nicholas; Halkias, Daphne y Sam Abadir. (2012). *e-Negotiations: Networking and Cross-Cultural Business Transactions*. Gower Publishing Limited, Farnham (Reino Unido).

Heilemann, John (Octubre 22, 2007). "When they were young." *New York Magazine*.

Henrikson, Alan K. (2013). "Sovereignty, Diplomacy, and Democracy: The Changing Character of 'International' Representation— from State to Self?"*The Fletcher Forum of World Affairs,* vol. 37, no.3, pp 111-140.

Hernández Gómez, José Ricardo. "Sun Tzu. El arte de la Guerra".*Revista virtual de inteligencia*. [En línea]. Disponible en: <http://revistadeinteligencia.es.tl/Sun-Tzu-d--Cap%EDtuloXIII.htm>. (Consulta 16/07/2013).

Herrera de Noble, Ernestina. (Enero 6, 2011). "Rebelión popular y masivo ataque de hackers en Túnez". *El Clarín*. [En línea]. Disponible en: <http://www.clarin.com/mundo/Rebelion-popular-masivo-hackers-Tunez_0_404359596.html>. (Consulta 21/05/2013).

Herrera Hermosilla, Juan Carlos. (2012).*Breve Historia del Espionaje*. Madrid: Nowtilus.

Hersh M., Seymour (Mayo 4, 2004). "Torture at Abu Ghraib". *The New Yorker*. [En línea] Disponible en: <http://www.newyorker.com/archive/2004/05/10/040510fa_fact>. (Consulta 10/03/2013).

Himma, Kenneth Einar. *Internet security: hacking, counterhacking, and society.*Jones and Bartlett. Estados Unidos, 2007.

Hildebrandt, Amber (Mayo 13, 2011). "Canada reconsidered Afghan combat end date: *WikiLeaks*". *CBC* News. En línea]. Disponible en: <http://www.cbc.ca/news/canada/canada-reconsidered-afghan-combat-end-date*WikiLeaks*-1.988520>. (Consulta 21/12/2013).

Hill, Gord (Mayo 4, 2011). "Wikileak Warriors: US cables on Native 'threats'". *Warrior Publications*. [En línea]. Disponible en: <http://warriorpublications.wordpress.com/2011/05/04/wikileak-warriors-us-cables-on-nativethrea>. (Consulta 21/12/2013).

Holburn,Chico LF; Berry, Dan; McNaught, Patrick; Moore, Michal y Jennifer Winter (Junio, 2013). "Wind Energy in Canada: A Survey of the Policy Environment". *Ivey Energy Policy and Management Centre*. [En línea]. Disponible en: <http://sites.ivey.ca/energy/files/2013/07/3554-Ivey-Energy-Wind-Policy-v04.pdf>. (Consulta 13/01/2014).

Howard, Philip N. (2006). *New Media Campaigns and the Managed Citizen*. Cambridge University Press, New York.

López, Miguel. (Septiembre 21, 2010). "*WikiLeaks*, todo lo que necesitas saber". *Genbeta*. [En línea]. Disponible en:<http://www.genbeta.com/activismo-online/*WikiLeaks*-todo-lo-que-n ecesitas-saber>. (Consulta 26/02/2013).

Ibarz, Mercè. (2005). "FOTOGRAFÍA Y GUERRA. LA IMAGEN DIGITAL COMO SÍNTOMA. LAS FOTOS DE ABU GHRAIB". *DOXA*, no. 3.[En línea] Disponible en: <http://www.uspceu.com/usp/doxa/doxaIII/6000%20DOXA%2007.pdf>. (Consulta 20/03/2013).

Information Warfare Monitor. (Marzo 29, 2009). *Tracking GhostNet: Investigating a Cyber Espionage Network*. Munk Centre for International Studies, University of Toronto. [En línea]. Disponible en: <http://www.nartv.org/mirror/ghostnet.pdf>. (Consulta 23/10/13).

Inglehart, Ronald. (1990). *Culture Shift in Advanced Industrial Society*.Princeton University Press, Princeton, NJ.

International Telecommunication Union. (Abril, 2014). *The World in 2014: ICT Facts and Figures*. [En línea]. Disponible en: <http://www.itu.int/en/ITU-D/Statistics/Documents/factsICTFactsFigures2014-e.pdf>. (Consulta 10/05/14).

International Multilateral Partnership against Cyber Threats. *About the Global Cybersecurity Agenda*. International Telecommunication Union. [En línea]. Disponible en: <http://www.impactalliance.org/aboutus>/ITU-IMPACT.html>. (Consulta 11/11/13).

Iprofesional. (Julio 1, 2013). "Con 4 notebooks, una llave USB y un cubo Rubik, Snowden destapó cómo funciona el espionaje mundial". *Emprendimientos Corporativos*. [En línea]. Disponible en: <http://www.iprofesional.com/notas/164134-Con-4-notebooks-una-llave-USB-y-un-cubo-Rubik-Snowden-destap-cmo-funciona-el-espionaje-mundial>. (Consulta 20/07/2013).

Irán Spanish Radio. (Diciembre 6, 2010). "Reacciones a las revelaciones de *WikiLeaks*". *IRIB*. [En línea]. Disponible en: <http://spanish.irib.ir/an%C3%A1lisis/art%C3%ADculos/item/110023-reacciones-a-las-revelaciones-de-*WikiLeaks*>. (Consulta 26/06/2013).

Islas, Octavio. *Explorando el ciberperiodismo iberoamericano*.Grupo Patria Cultural. México, 2002.

J. Paul B. De Taillon. (2001). The Evolution of Special Forces in Counter-terrorism: The British and American Experiences. Greenwood Publishing Group, Estados Unidos.

Jaff, Dave. (Enero, 2000). "Unitarians join Seattle protest against the WTO". *The Canadian Unitarian*, vol. 41, no. 1, pp. 1-2. [En línea]. Disponible en: <http://cuc.ca/wp-content/uploads/2011/10/January2000.pdf>. (Consulta 23/12/2013).

Jacobson, David. (Enero 21, 2010). 10OTTAWA29, Canada's Conservative Government and its Arctic Focus. *WikiLeaks*. [En línea]. Disponible en: <http://*WikiLeaks*.org/cable/2010/01/1 0OTTAWA29.html>. (Consulta 14/01/2014).

Jennings, M. y Zeitner, C. (2003). "Internet use and civic engagement." *Public Opinion Quarterly*, vol. 67. p. 311-334.

Johnson, Ian. (Marzo 19, 2003). "Canada in hacktivist crosshairs". *The Globe and Mail*. [En línea]. Disponible en: <http://www.theglobeandmail.com/technology/canada-in-hacktivist-crosshairs/article1158937/>. (Consulta 28/12/2013).

Juárez Valero, Eduardo. (Diciembre, 2012). "Espías y agentes dobles durante la Edad Media". Historia National Geographic, No. 109. [En línea]. Disponible en: <http://www.nationalgeographic.com.es/articulo/historia/secciones/7942/espias_agentes_dobles_durante_edad_media.html>. (Consulta 25/08/13).

Kaplan, Rubén. "*WikiLeaks* y Medio Oriente". *ANAJNU*. [En línea]. Disponible en: <http://www.anajnu.cl/wikimediooriente.htm>. (Consulta 02/06/2013).

Kaspersky Lab. (1996-2014). "Ataque DoS". *Viruslist.com*. [En línea]. Disponible en: <http://www.viruslist.com/sp/glossary?glossid =153602817>. (Consulta 26/12/2013).

Kaspersky Lab. (Enero 14, 2013). *"Red October" Diplomatic Cyber Attacks Investigation*. Securelist. [En línea]. Disponible en: <http://www.securelist.com/en/analysis/204792262/Red_October_Diplomatic_Cyber_Attacks_Investigation>. (Consulta 05/11/13).

Kelly, Martina. (2013). "Paul Baranowski, Software Developer". *CareerMash*. [En línea]. Disponible en: <http://careermash.ca/careers/meet-the-pros/paul-baranowski>. (Consulta 28/12/2013).

Keown, Leslie-Anne. (2007). "Keeping up with the times: Canadians and their news media diet." *Canadian Social Trends*, no. 82. [En línea]. Disponible en: <http://www.statcan.ca/bsolc/english/bsolc?catno=11-008-X2007003961>. (Consulta 28/12/2013).

Kilibarda, Konstantin. (2012). "Lessons from #Occupy in Canada: Contesting Space, Settler Consciousness and Erasures within the 99%". *Journal of Critical Globalisation Studies*, no. 5, pp. 24-41. [En línea]. Disponible en: <http://www.criticalglobalisation.com/issue5/24_41_OCCUPY_IN_CANADA_JCGS5.pdf>. (Consulta 26/12/2013).

King, Jonathan. (2009). "Intelligence Gathering of the Mongolian Empire". *Études Historiques*, 2009 ,vol. 1, no. 2. [En línea]. Disponible en: <http://www.etudeshistoriques.org/index.php/etudeshistorique/article/viewFile/7/7>. (Consulta 23/08/13).

Kingsmith, A. T. (2013). "Virtual Roadblocks: The Securitisation of the Information Superhighway". *Bridges: Conversations in Global Politics and Public Policy*, vol. 2, no.1. [En línea]. Disponible en: <http://digitalcommons.mcmaster.ca/cgi/viewcontent.cgi?article=1010&context=bridges>. (Consulta 10/02/2014).

Klein, Naomi. (Marzo 13, 2000). "My Mafiaboy". The Nation. [En línea]. Disponible en: <http://www.thenation.co m/article/my-mafiaboy#>. (Consulta 28/12/2013).

Kumon, Shumpei. "Japan as a Network Society", en Shumpei Kumon y Henry Rosovsky (eds.), *The Political Economy of Japan*, vol. 3, *Cultural and Social Dynamics*. Stanford University Press, Stanford, California, 1992, pp. 109-141.

Kurbalija J., Baldi S. (2000). Internet Guide for Diplomats. Malta: DiploPublishing Dumnn Cavelty, Myriam. *Cyber-Security and Threat Politics: Us Efforts to Secure the Information Age*. Routledge. Nueva York, 2008.

Laborie Iglesias, Mario. (Febrero, 2013). "Contratistas Privados y la sombra de Abu Ghraib". *Instituto Español de Estudios Estratégicos*. [En línea]. Disponible en: <http://www.ieee.es/Galerias/fichero/docs_analisis/2013/DIEEEA082013_Contratistas_AbuGhraib_MLI.pd>. (Consulta 3/03/2013).

LaSalle, LuAnn. (Febrero 13, 2013). "Hacktivists make their causes known online while masked in anonymity". The Winnipeg Free Press. [En línea]. Disponible en: <http://www.ctvnews.ca/sci-tech/hacktivists-make-their-causes-known-online-while-masked-in-anonymity-1.1155160>. (Consulta 28/12/2013).

Lascurain Huerta, Antonio. "Una borrosa fotocopia" *a.m.* [En línea]. Disponible en: <http://archivo.periodico.am/columna.aspx?id=16417>. (Consulta 28/01/2013).

Lauren, Paul Gordon. *Force and statecraft: diplomatic challenges of our time*. Oxford University Press. Nueva York, 2007.

Leigh, David y Luke Harding. *WikiLeaks, Inside Julian Assange´s War on Secrecy*. Guardianbooks. Reino Unido, 2011.

Lévy¸ Pierre. (2004). *Ciberdemocracia: Ensayo sobre Filosofia Politica*. Editorial UOC, Barcelona.

Levy, Steven. (2010). *Hackers: Heroes of the Computer Revolution*. O' Reilly Media, Inc. Estados Unidos.

Ley de Seguridad Nacional. [En línea]. Disponible en: <http://www.ordenjuridico.gob.mx/Federal/Combo/C-8.pdf>. (Consulta 24/05/2013).

Licklider, Robnett y Joseph Carl. (Marzo, 1960). *Man-Computer Symbiosis*. IRE Transactions on Human Factors in Electronics, volumen HFE-1, pp. 4-11. [En línea]. Disponible en: <http://sloan.stanford.edu/mousesite/Secondary/Licklider.pdfer.html>. (Consulta 12/02/2013).

Licklider, Robnett; Carl, Joseph y Robert W. Taylor. (Abril, 1968). *The Computer as a Communication Device*. Science and Technology. [En línea]. Disponible en: <http://sloan.stanford.edu/mousesite/Secondary/Licklider.pdf>. (Consulta 12/02/2013).

Lijphart, Arend. (1997). "Unequal participation: Democracy's unresolved dilemma."*American Political Science Review*, vol. 91, pp. 1-14.

Lipnack, Jessica y Jeffrey Stamps. (1994). *The Age of the Network*. Wiley & Sons, Nueva York.

Mandiant. *APT1, Exposing One of China's Cyber Espionage Units*. [En línea]. Disponible en: <http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf>. (Consulta 29/10/13).

Mandraud, Isabelle. (Enero 17, 2011). "En Tunisie, la révolution est en ligne". *Le Monde*. [En línea]. Disponible en: <http://www.lemonde.fr/afrique/article/2011/01/17/en-tunisie-la-revolution-est-en-ligne_1466624_3212.html>. (Consulta 20/06/2013).

Marcano, Edgar. (Noviembre 29, 2010). "Fugas de *WikiLeaks*: Lawrence Cannon no está preocupado". Despertar dominicano. [En línea]. Disponible en: <http://www.despertardominicano.com/noticias/noticias-de-canada/197-fugas-de*WikiLeaks*-lawrence-cannon-no-esta-preocupado>. (Consulta 21/11/2013).

Machlup, F. (1962). *The production and distribution of knowledge in the United States* (Vol. 278). Princeton university press, EE.UU.

Matterlart, Armand. (2002). *Historia de la Sociedad de la Información.*Paidós Ibérica, España.

Matterlart, Armand. (1998). *La mundialización de la comunicación*. Paidós, Barcelona.

May, Christopher. (2003). *Key Thinkers for the Information Society: Volume One*, Routledge Nueva York.

Mearian, Lucas. (Junio 4, 2013). "The next corporate revolution will be power to the peons". *Computerworld*.

Melgar Valero, Luis Tomás. (2010). *Diplomacia pública: la gestión de la imagen-país. El modelo español*. Ministerio de Asuntos Exteriores y de Cooperación,Madrid.

McDonald, Matt. (2008). *Securitization and the Construction of Security en European Journal of International Relations,* vol. 14(4), 2008.

McLuhan, Eric. (1996). "The source of the term 'global village'". *McLuhan Studies*, no. 2.

Milan, Stefania y Arne Hintz. (Marzo 15, 2013). "Networked Collective Action and the Institutionalized Policy Debate: Bringing Cyberactivism to the Policy Arena?"*Policy and Internet*, vol. 5, no. 1, pp. 7-25. [En línea]. Disponible en: <http://onlinelibrary.wiley.com/doi/10.1002/poi3.20/pdf>. (Consulta 24/01/2014).

Milecki, Andrzej. "Schulmeister Karl Ludwig (1770 - 1853)". *Napoleon.org.pl.* [En línea]. Disponible en: <http://www.napoleon.org.pl/polityka/schul.php>. (Consulta 30/08/13).

Miller, Gerry; Sinclair, Gerri; Sutherland, David y Julie Zilber (Marzo, 1999). *Regulation of the Internet. A technological Perspective.* Spectrum Management and Telecommunications. [En línea]. Disponible en: <http://www.ic.gc.ca/eic/site/smt-gst.nsf/vwapj/05082eng.pdf/FILE/05082-eng.pdf>. (Consulta 28/01/2014).

Miller, Jeff. (2012). "Net-Neutrality Regulation in Canada: Assessing the CRTC's Statutory Competency to Regulate the Internet". *APPEAL*, vol. 17, pp. 47-62. [En línea]. Disponible en: <http://journals.uvic.ca/index.php/appeal/article/viewFile/11888/3372>. (Consulta 28/01/2014).

Miller, John y Cybele Sack. Terrorism and Anonymous Sources: The Toronto 18 Case. Ryerson University. [En línea]. Disponible en: <http://cjms.fims.uwo.ca/issues/08-01/Toronto_18.pdf>. (Consulta 20/11/2013).

Miller Jones, Edward R. (2010). *WikiLeaks, Removing the 'top secret' seal.* Estados Unidos: Fastbookpublishing.

Moore, Malcolm. (Abril 6, 2010). "Chinese hackers steal Dalai Lama's emails". *The Telegraph.* [En línea]. Disponible en: <http://www.telegraph.co.uk/news/worldnews/asia/china/ 7559 103/Chinese-hackers-steal-Dalai-Lamas-emails.html>. (Consulta 23/10/13).

Morris, Nigel. (Junio 7, 2013). "Q&A: What is Prism, what does it do, is it legal and what data can it obtain?"*The Independent*. [En línea]. Disponible en: <http://www.independen t.co.uk/news/world/americas/qa-what-is-prism-what-does-it-do-is-it-legal-and-what-data-can-it-obtain-8650239.html>. (Consulta 10/11/13).

Muñoz, Alonso. (2010). "*WikiLeaks*, mucho más que Julian Assange". Diagonal. [En línea]. Disponible: <http://www.diagonalperiodico.net/*WikiLeaks*-mucho-ma-s-que-Julian.html>. (Consulta 11/05/2014).

Navarro Bonilla, Diego. (2005). "Información, Espionaje e Inteligencia en la Monarquía hispánica (Siglos XVI-XVII)". Revista de historia militar, pp. 13-34. [En línea].

Disponible en: <http://www.portalcultura.mde.es/Galerias/revistas/ficheros/RHM_servicios informacionmodernos.pdf>. (Consulta 11/08/2013).

Nelson, Marissa. (Mayo 11, 2011). "Photo Galleries Charest defends against *WikiLeaks* report". *CBC News*. [En línea]. Disponible en: <http://www.cbc.ca/news/canada/montreal/charest-defends-against-*WikiLeaks*-report-1.105 8273>. (Consulta 14/01/2014).

Nelson, Marissa. (Noviembre 28, 2010). "*WikiLeaks* reveals undiplomatic U.S. critiques". CBC News. [En línea]. Disponible en: <http://www.cbc.ca/news/world/*WikiLeaks*-reveals-undip lomatic-u-s-critiques-1.878000>. (Consulta 26/11/2013).

Nelson, Marissa. (Junio 6, 2011). "*WikiLeaks* shows bitter Canada-U.S.". *CBC News*. [En línea]. Disponible en: <http: //www.cbc.ca/news/canada/manitoba/*WikiLeaks*-shows-bitter-canada -u-s-water-tiff-1.1073888>. (Consulta 13/12/2014).

Neuman, Peter G. (Enero, 1984). *Software engineering notes*. Association for Computing Machinery, vol. 111, no. 5.

Neuman, Russell. (1999). "The Global Impact of new technologies". En: Graber, Doris; Mc quail, Dennis y Pippa Norris (Eds.). *The Politics of News. The news of Politics*. Washington, Dc: CQ Press.

Newfoundland and Labrador. (Enero 10, 2014). "Open Custody". *Departament of Child, Youth and Family Services*. [En línea]. Disponible en: <http://www.gov.nl.ca/cyfs/youthcorrecti ons/opencustody.html>. (Consulta 27/12/2013).

Niemi, Richard G. y Herbert F. Weisberg (eds.) (2001). *Controversies in Voting Behavior*. CQ Press, Washington, D.C.

Noble, Joshua. (Junio 2, 2011). "*WikiLeaks*, Canadian media and democracy: Media with a face". *The Toronto Star*. [En línea]. Disponible en: <http://www.thestar.com/opinion/edit orialopinion/2011/06/02/*WikiLeaks*_canadian_media_and_democracy_media_with_a_fac e.html>. (Consulta 27/01/2014).

Norris, Pippa. (1999). *Who Surfs? New Technology, Old Voters and Virtual Democracy*. En Kamarck, Ciulla Elaine y Joseph Nye Jr. (eds.). *Democracy.com? Governance in a Networked World*. Hollis Publishing. Hollis, NH, pp. 71-94.

North Atlantic Treaty Organization. (Octubre 22, 2013).*NATO and cyber defence*. [En línea] Disponible en: <http://www.nato.int/cps/en/natolive/topics_78170.htm?>. (Consulta 20/11/13).

Notimex. (Febrero 1, 2011). "Convocan a reunión masiva de embajadores de EU; Egipto y *WikiLeaks*, causas". *Criterio Hidalgo*. [En línea] Disponible en: <http://www.criteriohida lgo.com/notas.asp?id=36152>. (Consulta 24/05/2013).

Notimex. (Marzo 22, 2011). "Renuncia de Carlos Pascual fue 'decisión personal': EU". *La Jornada.* [En línea]. Disponible en: <http://www.jornada.unam.mx/2011/03/22/politica/006nlpol>. (Consulta 02/02/2013).

Notimex. (Junio 3, 2013). "Turquía vive tercera jornada de violentas protestas". *El Universal.* [En línea]. Disponible en: <http://www.eluniversal.com.mx/notas/927100.html>. (Consulta 28/04/2013).

Nowotny, Thomas. (2011). *Diplomacy and Global Governance, The diplomatic service in an Age of Worldwide Interdependence.* TransactionPublishers. EE.UU.

Nweke, Eugene. (2012). "Diplomacy in Era of Digital Governance: Theory and Impact". *Information and Knowledge Management*, vol. 2, no. 3, pp. 22-27. [En línea]. Disponible en: <http://www.iiste.org/Journals/index.php/IKM/article/viewFile/1784/1737>. (Consulta 6/02/2014).

Nye, Joseph Jr. (2003). *La paradoja del poder norteamericano.* Taurus. Madrid.

Olive, David. (Abril 8, 2007). "Rumours of newspapers' demise". *The Toronto Star.* [En línea]. Disponible en: <http://www.thestar.com/Business/article/200650>. (Consultada 13/08/2013).

ONCEAVA REUNIÓN DEL COMITÉ ESPECIAL DEL SENADO EN ANTI-TERRORISMO (11: 2010: Ottawa). Tercera sesión del cuadragésimo Parlamento de Canadá. Ottawa: Diciembre 6, 2010. [En línea]. Disponible en: <http://www.parl.gc.ca/Content/SEN/Committee/403/anti/48515e.htm?comm_id=597&Language=F&Parl=40&Ses=3>. (Consultada 15/01/2014).

Organización de Estados Americanos. (Junio 8, 2004).*Estrategia de seguridad cibernética (RESOLUCION).* Comité Interamericano contra el Terrorismo. [En línea]. Disponible en: <http://www.oas.org/es/ssm/cyber/documents/Estrategia-seguridadciberneticaresolucion.pdf>. (Consulta 11/11/13).

Organización de Naciones Unidas. (Abril 12-19, 2010).*12º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal.* (Nota 32 y 33). [En línea] Disponible en: <http://www.unodc.org/documents/crimecongress/12thCrimeCongress/Documents/A_CONF.213_9/V1050385s.pdf>. (Consulta 11/11/13).

Organización de Naciones Unidas. "Décimo Congreso de las Naciones Unidas sobre Prevención del Delito y Tratamiento del Delincuente Viena, 10 a 17 de abril de 2000".*Naciones Unidas*, Nueva York, p. 6. [En línea] Disponible en: <http://www.uncjin.org/Documents/congr10/15s.pdf>. (Consulta 2/06/2013).

Organización de Naciones Unidas y Unión Internacional Telecomunicaciones.(2003). "Declaración de Principios, Construir la Sociedad de la Información: un desafío global para el nuevo milenio". *Cumbre Mundial sobre la Sociedad de la Información Ginebra 2003 – Túnez* 2005, p.8. [En línea]. Disponible en: <http://www.itu.int/wsis/docs/geneva/official/dop-es.html>. (Consulta 02/06/2013).

Organización para la Cooperación y el Desarrollo Económicos. "Bribery in international business". [En línea]. Disponible en: <http://www.oecd.org/daf/anti-bribery/>. (Consulta 13/07/13)

Organización para la Cooperación y el Desarrollo Económicos. (2006). *Directrices de la OCDE para la seguridad de sistemas y redes de información: Hacia una cultura de seguridad*. Ministerio de Administraciones Públicas y Secretaría General Técnica. España. [En línea] Disponible en: <http://www.oecd.org/internet/ieconomy/34912912.pdf>. (Consulta 11/11/13).

Parreño, Antonio. (Enero 3, 2012). "El chico que se quemó e incendió el mundo árabe". *Rtve.* [En línea]. Disponible en: <http://www.rtve.es/noticias/20120103/mohamed-bouazizi-chico-no-pudomas/482545.shtml>. (Consulta 29/05/2013).

Pérez Silva, Ciro. (Julio 3, 2012). "México trata de manera directa con EU las 'presuntas filtraciones': SRE". *La Jornada*, p. 3.

Petrella, R. (1993). "Vers un techno-apartheid global". *Manières de voir- Le Monde Diplomatique,* no.18.

Political Culture Researchomatic (Diciembre, 2011). *Social Movements in Canada.* [En línea]. Disponible en: <http://www.researchomatic.com/Political-Culture-98036.html>. (Consulta 23/12/2013).

Prolexic (2003-2014). "What is DDoS denial of service?"*Knowledge Center.* [En línea]. Disponible en: <http://www.prolexic.com/knowledge-center-what-is-ddos-denial-ofservice.html>. (Consulta 27/12/2013).

Putman, Robert. (2000). *Bowling Alone: The collapse and Revival of American Community*. Simon y Schuster, Nueva York.

Putnam, Robert (2004). *Education, Diversity, Social Cohesion and Social Capital*. Note for discussion, Meeting of OECD Education Ministers, March 18-19, Dublin. [En línea]. Disponible en: <www.oecd.org/dataoecd/37/55/30671102.doc>. (Consulta 11/08/2008).

Qingshan, Li. (1995). New *Military Revolution and High Tech War.* Beijing: AMS Press.

Qingsong, Wang. (1993).*Modern Military-Use High Technology*. Beijing: AMS Press.

QuebécLeaks. (2013). *What is QuebécLeaks?* [En línea]. Disponible en: <https://www.quebecleaks.org/en/about-us/what-is-quebecleaks/>. (Consulta 28/12/2013).

Quesada Pérez, Montserrat. (1998). *Periodismo Especializado*. Ediciones Internacionales Universitarias S.A., Madrid.

QUINTA REUNIÓN DEL COMITÉ PERMANENTE DEL SENADO SOBRE SEGURIDAD NACIONAL Y DEFENSA (5: 2012: Ottawa). Tercera sesión del cuadragésimo Parlamento de Canadá. Ottawa: Marzo 26, 2012. [En línea]. Disponible en: <http://www.parl.gc.ca/content/sen/committee/411%5CSECD/05EVA-49438-e.HTM>. (Consulta 14/03/2014).

Radio-Canada (Mayo 11, 2011). "Charest se défend d'être influencé par Power Corp.". *CBC News*. [En línea]. Disponible en: <http://www.radio-canada.ca/nouvelles/Politique/2011/05/11/003-charest-powercorp-wikilaks.shl>. (Consulta 14/01/2014).

Ramírez, Pedro J. (Noviembre 30, 2010). "Julian Assange podría ser procesado de acuerdo a la Ley de Espionaje". *El Mundo*. [En línea]. Disponible en: <http://www.elmundo.es/america/2010/11/30/estados_unidos/1291142768.html>. (Consulta 23/04/2013).

Richelson, Jeffery T. (1995). *A Century of Spies Intelligence in the Twentieth Century*. Nueva York: Oxford University Press.

Rodham Clinton, Hillary. (Enero 21, 2010). *Discurso sobre libertad en Internet*. Museo de la Información Newseum, Washington DC. [En línea].Disponible: <http://www.state.gov/documents/organization/135880.pdf>. (Consulta 16/05/2013).

Rosas Lauro, Claudia (ed.) (2005).*El miedo en el Perú: siglos XVI al XX*. Perú: Fondo Editorial.

Rose, Alexander. (Julio 15, 1998). "Terror has a New Name: Internet". *The National Post.*

Roy, Jeffrey. (2006). *E-Government in Canada: Transformation for the Digital Age*. University for Ottawa Press, Canadá.

RT. (2012). "Diálogos con Assange". *TV-Novosti*, capítulo 6. [En línea]. Disponible en: <http://assange.rt.com/es/el-mundo-del-maana-episodio-5-assange-y-correa-la-esperada-entrevista-en-rt/full-translation-text/#page-1>. (Consulta 03/07/2013).

RT. (Julio 27, 2010). "Los informes clasificados de *WikiLeaks* despiertan a Amnistía Internacional". *TV-Novosti*. [En línea]. Disponible en: <http://actualidad.rt.com/video/actualidad/view/70643-Los-informes-clasificados-de-*WikiLeaks*-despiertan-a-Amnist%C3%ADaInternacional>. (Consulta 12/05/2013).

Rubio, Rafael. (2011). *Diplomacia digital. Una introducción.* En *Las relaciones internacionales en el tránsito al siglo XXI.* Cuadernos de la Escuela Diplomática, no. 44. Escuela Diplomática y Ministerio de Asuntos Exteriores y Cooperación. España, pp. 19-56.

Rudner, Martin. (2013). "Cyber-Threats Critical National Infrastructure: An Intelligence Challenge". *International Journal of Intelligence and CounterInterlligence.* Routledge, Vol. 26, no. 3, pp. 453-481.

Ruffin, Oxblood. (Julio 15, 1998). "The Longer March: Interview with Blondie Wong". *cDc communications #356.* [En línea]. Disponible en: <http://www.cultdeadcow.com/cDc_files/cDc-0356.html>. (Consulta 28/12/2013).

Salas, Antonio. (2010).*El Palestino.* Planeta Madrid, España.

Sánchez Hernández, Carlos. (Marzo, 2011). "Analogías de la Historia I: Julian Assange y *WikiLeaks* vs Daniel Ellsberg y los Pentagon Papers". *Nómadas. Revista Crítica de Ciencias Sociales y Jurídicas*, no. 31. [En línea]. Disponible en: <http://pendientedemigracion.ucm.es/info/nomadas/31/carlosschzhernandez.pdf>. (Consulta 11/11/2013).

Sánchez Hernández, Carlos. (2005). "Treinta años después del Watergate (1974-2004)".*Nómadas.* [En línea].Disponible en:<http://www.redalyc.org/articulo.oa?id=18101106>. (Consulta 21/02/2013).

Sanou, Brahima. (2013). "The World in 2013 - ICT Facts and Figures". *ITU.* [En línea] Disponible en: <http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2013.pdf>. (Consulta 02/06/2013).

Schulting, Rick J. y Linda Fibiger (edit.). (2012). *Sticks, Stones, and Broken Bones: Neolithic Violence in a European Perspective.* Reino Unido: Oxford.

Secretaría de Gobernación. *Denuncia Delitos Cibernéticos*. Comisión Nacional de Seguridad. [En línea]. Disponible en: <http://www.ssp.gob.mx/portalWebApp/ShowBinary?nodeId=/BEA%20Repository/1276161>. (Consulta 11/11/13).

Security Service. (2012). "M16". *Politics.co.uk.* [En línea]. Disponible en: <http://www.politics.co.uk/reference/mi6>. (Consulta 25/09/13).

Shah, D., J. McLeod y S. Yoon (2001). "Communication, context, and community: An exploration of print, broadcast, and Internet influences." *Communication Research*, vol. 28, no. 4. p. 464-506.

Shenglong, Dai y ShenFuzhen. (1996).*Information Warfare and Information Security Strategy.* Beijing: Jincheng Publishing House.

Shubert, Atika; Ashley Frantz y Moni Basu. (Diciembre 3, 2010). "La vida secreta de Julian Assange, el fundador de *WikiLeaks*". Sección: El efecto *WikiLeaks*. CNN México. [En línea]. Disponible: <http://mexico.cnn.com/mundo/2010/12/03/la-vida-secreta-de-julian-assange-el-fundador-de-*WikiLeaks*>. (Consulta 11/ 03/2014).

Shulgan, Christopher (Diciembre 19, 2002). "Ottawa Citizen Profile of the Citizen Lab and HACKTIVISM". *Citizenlab*. [En línea]. Disponible en: <https://citizenlab.org/2002/12/ottawa-citizen-profile-of-the-citizen-lab-and-hacktivism/>. (Consulta 27/12/2013).

Sciadas, George (2006). "Our lives in digital times." *Connectedness Series,* no. 14. [En línea]. Disponible en: <http://www.statcan.ca/bsolc/english/bsolc?catno=56F0004M2006014>. (Consulta 12/08/2008).

Simkin, John. "Military Intelligence (MI6)". *Spartacus Educational*. [En línea]. Disponible en: <http://www.spartacus.schoolnet.co.uk/FWWm6.htm>. (Consulta 25/09/13).

Statistics Canada (Junio 12, 2008). *Canadian Internet Use Survey*. [En línea]. Disponible en: <http://www.statcan.ca/Daily/English/080612/d080612b.htm>. (Consulta 12/01/2013).

Statistics Canada (2006). *The daily: Canadian Internet use survey*. [En línea]. Disponible en: <http://www.statcan.gc.ca/daily-quotidien/060815/dq060815b-eng.htm>. (Consulta 15/01/2014).

Statistics Canada. (Noviembre 26, 2013). *Canadian Internet Use Survey, 2013*. [En línea]. Disponible en: <http://www.statcan.gc.ca/daily-quotidien/131126/dq131126d-eng.pdf>. (Consulta 11/05/2014).

Stiennon, Richard. (2010).*Surviving Cyberwar*. Government Institutes, Estados Unidos.

Sun Tzu. (2005). *El arte de la guerra*. México: Leyenda.

Suáres, Luis E. (Marzo 13, 2005). "General Reinhard Gehlen". *Exordio*. [En línea]. Disponible en: <http://www.exordio.com/1939-1945/militaris/espionaje/gehlen.html>. (Consulta 05/11/13).

Tapscott, Don y Anthony Williams. (2010). *Macrowikinomics*. Penguin, Toronto.

Tapscott, Don y David Agnew. (Diciembre, 1999). "Governance in the Digital Economy". *Finance and Development*, pp. 84-87.

Telecommunication Standardization Advisory Group. (Octubre 4, 2004).*Cybersecurity Symposium*. International Telecommunication Union. [En línea]. Disponible en: <http://www.itu.int/ITU-T/worksem/cybersecurity/>. (Consulta 11/11/13).

The Associated Press (Diciembre 1, 2010). "Flanagan regrets *WikiLeaks* assassination remark". *CBC News*. [En línea]. Disponible en: <http://www.cbc.ca/news/politics/flanagan-regrets-*WikiLeaks*-assassination-remark-1.877548>. (Consulta 11/12/2013).

The Avalon Proyect, Documents in Law, History and Diplomacy. *Anti-Comintern Pact.*Yale Law School. [En línea]. Disponible en: <http://avalon.law.yale.edu/wwii/tri1.asp>. (Consulta 10/09/13).

The Canadian Press (Diciembre 3, 2010). "*WikiLeaks* founder calls for Flanagan charge". *CBC News*. [En línea]. Disponible en: <http://www.cbc.ca/news/politics/*WikiLeaks*-foundercalls -for-flanagan-charge-1.877546>. (Consulta 26/12/2013).

The Canadian Press (Mayo 12, 2011). "*WikiLeaks*: U.S. dismisses Harper's Arctic talk". *CBC News*. [En línea]. Disponible en: <http://www.cbc.ca/news/canada/*WikiLeaks*-u-s-dismisse s-harper-s-arctic-talk-1.1009886>. (Consulta 13/01/2014).

Trinity-hackers (2013). "The Hong Kong Blondes". *Creative Commons Attribution Share-Alike.* [En línea]. Disponible en: <http://trinity-hackers.wikispaces.com/The+Hong+Kong+Blon des>. (Consulta 27/12/2013).

Tooze, R.I. (1978). "Communications Theory". En: Trevor Taylor (ed.*) Approaches and Theory in International Relations.*Longman Tversky, Amos y Daniel Kahneman, London.

Ulloa, Karina G. (Octubre 23, 2013). "Eurocámara cancela datos bancarios para EE.UU". *Sexenio*. [En línea]. Disponible en: <http://www.sexenio.com.mx/articulo.php?id=4014>. (Consulta 20/11/13).

Unión Europea. (2004). "Retos para la sociedad de la información europea con posterioridad a 2005".*Comisión de las Comunidades Europeas*, p. 7. [En línea]. Disponible en: <http://europa.eu/legislation_summaries/information_society/strategies/l24262_es.htm>. (Consulta 03/06/2013).

Unión Internacional de Telecomunicaciones. (Octubre 7, 2013). *La UIT publica las cifras técnicas y clasificaciones mundiales más recientes. Ginebra, Suiza*. [En línea]. Disponible en: <http://www.itu.int/net/pressoffice/press_releases/2013/41-es.aspx #.U261OoF5PHo>. (Consulta 10/05/2014).

Valeri, Lorenzo. (2007).*Public-private cooperation and information assurance*. En Eriksson, Johan y Giampiero Giacomello. *International Relations and Security in the Digital Age*. (pp. 132-157) Londres: Routledge.

Van Creveld, Martin. (1991). *Technology and War: From 2000 B.C. to the Present*. Estados Unidos: The Free Press.

Veenhof, Ben (Mayo 15, 2006). *Determinants and Outcomes of Heavy Computer Use: An International and Interprovincial Comparison.* Presentación de *Statistics Canada* en la Conferencia Socio-económica de Gatineau, Quebéc.

Veenhof, Ben; Wellman, Barry; Quell, Carsten y Bernie Hogan (Diciembre 4, 2008). *How Canadians' Use of the Internet Affects Social Life and Civic Participation.* Statistics Canada. [En línea]. Disponible en: <http://www.statcan.gc.ca/pub/56f0004m/56f0004m2008016-eng.pdf>. (Consulta 28/12/2013).

Viana, Israel. (Octubre 2, 2013). "Harry Gold, el espía 'rechoncho' que entregó la bomba atómica a la URSS". *ABC.es*. [En línea]. Disponible en: <http://www.abc.es/20101210/archivo/harry-gold-espia-entrego-201012091242.html>. (Consulta 20/10/13).

Villalobos R., Sergio *et al.* (1999). *Historia del pueblo chileno* (Tomo IV). Santiago De Chile: Editorial Universitaria.

Wau Holland Stiftung. (2012). *WikiLeaks*/Project 04: Monthly Balance 2010-2012.Wauland. [En línea]. Disponible: <http://www.wauland.de/files/2010-2012_Projekt04-Balance.pdf>. (Consulta 11/05/2014).

Weiguang, Shen. (1997).*On New War*. Beijing: Renminchubanshe.

Weston, Greg. (Febrero 16, 2011). "Foreign hackers attack Canadian government".*CBCnews*. [En línea]. Disponible en: <http://www.cbc.ca/news/politics/foreign-hackers-attackcanadian-government-1.982618>. (Consulta 29/10/13).

Wilson, Christopher. (Octubre13-15, 2013). "Internet Will Make Governments Unrecognnizable by Today´s Standards: From Leadership to Stewardship and Collaboration." Acta del *Segundo Foro Internacional de Ciencias Sociales*, Universidad de Ottawa. Montreal. [En línea]. Disponible en: <http://www.christopherwilson.ca/papers/The_Internet_will_make_governments_unrecognizable.pdf>. (Consulta 10/02/2014).

WikiLeaks. (Julio 25, 2010). *Afghan War Diary, 2004-2010.* [En línea]. Disponible en: <http://*WikiLeaks*.org/wiki/Afghan_War_Diary,_2004-2010>. (Consulta 15/04/2013).

WikiLeaks. (Enero 25, 2008). "Primetime Images of US-Canada Border Paint U.S. In Increasingly Negative Light". *Cablegatesearch.net.* [En línea]. Disponible en: <http://www.cablegatesearch.net/cable.php?id=08OTTAWA136&q=08ottawa136>. (Consulta 20/11/2013).

WikiLeaks. (Febrero 2, 2009). *Reporte RS21666.* [En línea]. Disponible en: <http://wlstorage.net/file/crs/RS21666.pdf>. (Consulta 16/01/2013).

WikiLeaks (Noviembre 13, 2013). *Secret TPP treaty: Advanced Intellectual Property chapter for all 12 nations with negotiating positions*. [En línea]. Disponible en: <http://*WikiLeaks*.org/tpp/static/pdf/*WikiLeaks*-secret-TPP-treaty-IP-chapter.pdf>. (Consulta 10/12/2013).

WikiLeaks. (2013).*Should the press really be free?* [En línea]. Disponible en: <http://*WikiLeaks*.org/About.html>.(Consulta 29/06/2013).

WikiLeaks. (2010). *Secret US Embassy Cables*. [En línea]. Disponible en: <https://*WikiLeaks*.or>. (Consulta 13/03/2014).

WikiLeaks (2014). "*WikiLeaks* Canada". Cablegateseach. [En línea]. Disponible en: <http://www.cablegatesearch.net/search.php?q=canada &sort=1>. (Consulta 27/12/2013).

Wilmoth Lerner, Adrienne. *Abwehr*.Espionage Information. Encyclpedia of Espionage, Intelligence and Security. [En línea]. Disponible en: <http://www.faqs.org/espionage/AA/Abwehr.html>. (Consulta 10/09/13).

Winseck, Dwayne. (2001). "Lost in Cyberspace: Convergence, Consolidation and Power in the Canadian Mediaescape". Ponencia presentada en *The Canadian Communications Association Annual Conference*. Quebec.

Xenos, Michael y Patricia Moy (2007). "Direct and differential effects of the Internet on political and civic engagement." *Journal of Communication*, vol. 57, p. 704-18.

Xiaoli, Zhu y Zhao Xiaozhuo. (1996). *The United States and Russia in the New Military Revolution*. Beijing: AMS Press.

59 ª REUNIÓN DEL COMITÉ PERMANENTE DE FINANZAS (59: 2011: Ottawa). Tercera sesión del cuadragésimo Parlamento de Canadá. Ottawa: Febrero 17, 2011. [En línea]. Disponible en: <http://www.parl.gc.ca/HousePublications/Publication.aspx?DocId=4977520&Language=E&Mode=1>. (Consulta 10/01/2014).

.