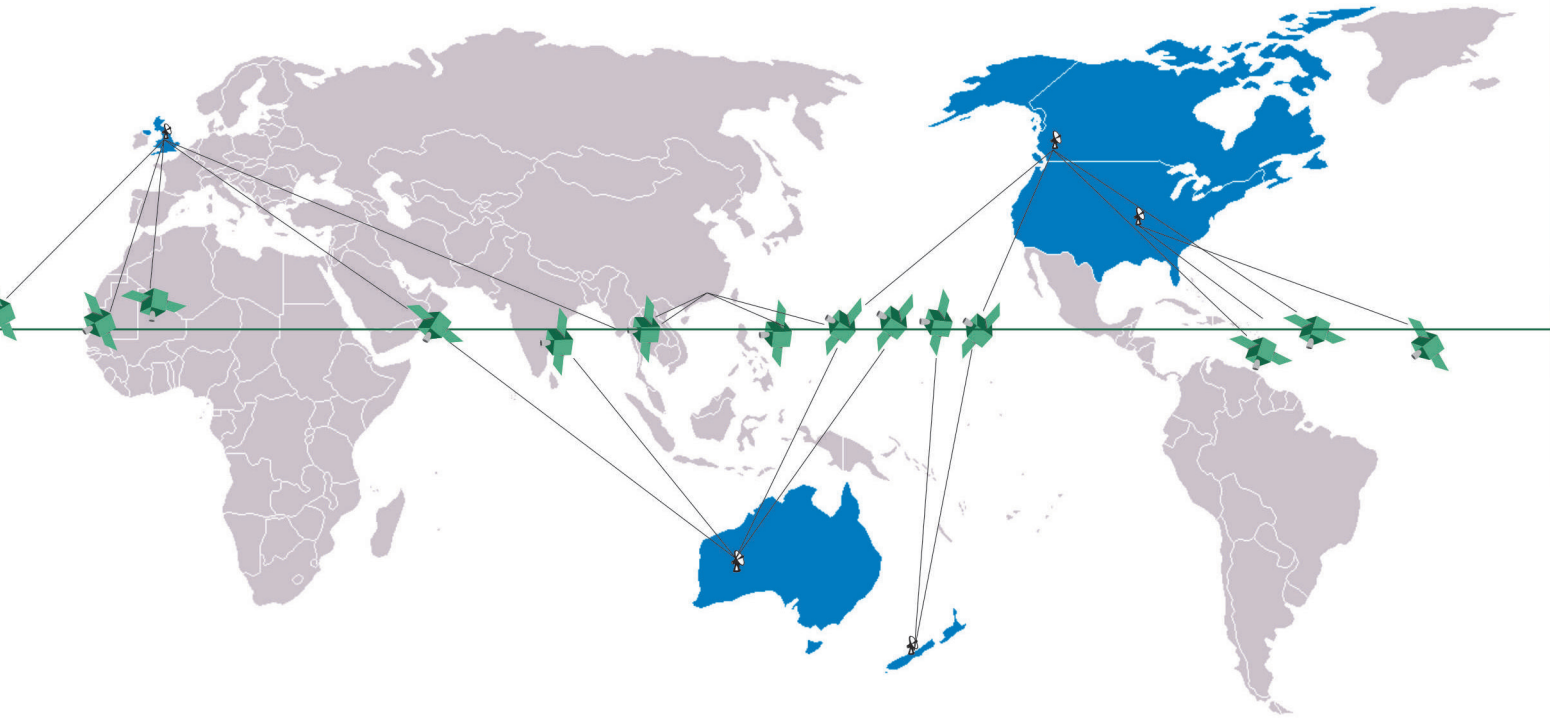


LA ALIANZA

UKUSA

EN INTELIGENCIA DE SEÑALES:

DE LOS ÉXITOS EN LA INTELIGENCIA ARTESANAL AL FRACASO DE LA MASIVIDAD.

1.3

José Gabriel Paz

Director del Instituto de Investigaciones en Geopolítica, Defensa y Seguridad de la Universidad del Salvador (Argentina), Director del Master en Defensa y Seguridad Hemisférica (USAL-CID, Washington DC), Director del Master en Defensa y Seguridad Centroamericana (USAL-CDN, Honduras), Asesor del Center for Latin American Economy and Trade Studies del Chihlee Institute of Technology de la Republica de China.

RESUMEN

La historia de la Alianza para inteligencia de señales UKUSA, -conformada por Estados Unidos, Reino Unido, Canadá, Australia y Nueva Zelanda-, muestra los éxitos y fracasos de una estructura de inteligencia multinacional, sostenida en base a una comunidad de intereses y la sólida lealtad entre sus miembros. El crecimiento de la tecnología ha generado la automatización, los procesos de búsqueda y obtención de la información, lo que ha tenido como consecuencia el desarrollo de programas de inteligencia cibernética, que al ser descubiertos han quedado en entredicho.

Consideraciones previas

Los crecientes avances en materia de tecnología de los últimos tiempos y particularmente los producidos en el campo de la informática, han multiplicado la capacidad de acceder con cierta facilidad a todo tipo de comunicación e información, sean de naturaleza militar, diplomática, científica o de los individuos en general.

Esta explosión tecnológica le ha dado a los países mayor aptitud para establecer con relativa certeza las características, capacidades e intenciones de sus posibles oponentes. En este contexto la inteligencia de señales (SIGINT) adquiere gran relevancia, puesto que al acceder al espectro de las comunicaciones es posible develar aspectos importantes sobre sus probables acciones. Exponiendo lo que hacen, lo que harán y lo que expresan, todo lo eventual permitirá una oportuna alerta sobre su actividad inminente.

Como cualquier actividad de inteligencia, las operaciones de SIGINT son ocultas al conocimiento público y se realizan con un alto grado de sigilo. Lo que hace difícil a los países detectarlas y establecer las oportunas contramedidas, y por esa razón no es frecuente atribuir a un país determinado la titularidad de una acción en este tipo de operaciones. Excepcionalmente se puede saber de ellas, sea por disponer la tecnología adecuada para su detección, a través de documentos desclasificados por los gobiernos o por infidencias de agentes y defectores.

Por décadas, las actividades de cooperación secretas en SIGINT de la comunidad de inteligencia UKUSA, -conformada por Estados Unidos, Reino Unido, Canadá, Australia y Nueva Zelanda- se han realizado en secreto. Sin embargo, en los últimos años se difundió a la prensa por parte de defectores, miles de documentos que develan sofisticadas operaciones llevadas a cabo por esa comunidad de inteligencia.

Esta situación, por sus superlativas consecuencias, merece su estudio dado las importantes implicancias que tiene en diversos campos. Por ello, a pesar de las naturales restricciones de acceso a fuentes de información, la complejidad de las tecnologías empleadas y necesidad de abreviar en aspectos históricos y técnicos, se buscará mostrar desde un contexto amplio. Algunas perspectivas sobre el empleo masivo de la inteligencia de señales, el protagonismo que le cabe a la comunidad UKUSA en esa tarea y sus resultados.

Los acuerdos de cooperación angloestadounidense en Sigint

La cooperación entre Estados Unidos y el Reino Unido en materia de inteligencia de señales se inicia informalmente en la Primera Guerra Mundial, consolidándose a través de acuerdos durante la Segunda Guerra Mundial.

En su desarrollo histórico se perciben y distinguen dos diferentes etapas en su forma de operar. La primera mayormente artesanal, va desde la Primera Guerra Mundial hasta el fin de a Guerra Fría, donde la actividad se centra en la capacidad de sus recursos humanos para la intercepción de comunicaciones y el criptoanálisis, y progresivamente se va agregando mayor tecnología; sumándose satélites, aviones, buques y estaciones de apoyo. La segunda etapa se extiende desde el fin de la Guerra Fría a nuestros días, donde con la pretensión de abarcar una universalidad de objetivos. Gran parte de la actividad se concentra en el uso masivo de la tecnología.

Sin pretender incursionar en profundidad sobre la historia de las estructuras de SIGINT de ambos países, puede decirse que desde fines del siglo XIX el Reino Unido, disponía de capacidades de interceptación y decodificación del correo postal, telegramas, señales Morse, así como la intervención de redes de telefonía y telégrafo[2] .

En 1914 el Almirantazgo británico crea la unidad de criptoanálisis llamada “Room 40” conocida como “40

O.B." (Old Building) y más tarde como "NID25", mientras que el ejército inglés forma la "Military Intelligence - Section 1b" o MI1b[3]. El 1 de noviembre de 1919 nace el "British Government Code and Cypher School[4]" (GC&CS). Conformado por las unidades MI1b y la "Room 40", manteniéndose hasta junio de 1949 cuando cambia su denominación por "Government Communications Headquarters" (GCHQ), cuyo nombre conserva hasta nuestros días.

La evolución de las agencias de inteligencia de señales de Estados Unidos fue más compleja, ya que desde sus inicios fueron cambiando de denominación y de dependencia orgánica.

Los orígenes de la inteligencia norteamericana se remonta a los tiempos de la Guerra Civil, pero la primera organización de SIGINT se crea a los pocos días de ingresar a la Primera Guerra Mundial. El 28 de abril de 1917 se funda la "Cipher Bureau and Military Intelligence Branch - Section 8" (MI-8) como parte del servicio de "Cable and Telegraph", la que luego se integrará a la Armada, conformando la "Code and Signal Section" (Op-20-G) dependiente del "Office of Chief Of Naval Operations" (OCNO), y se mantendrá con diferentes nombres hasta 1946, momento en que se suma a otras unidades de inteligencia naval.

En 1929 se crea el "Signal Intelligence Service" (SIS) que en junio de 1942 cambia de nombre a "Signal Intelligence Service Division" (SISD). Un mes después fue designado como "Signal Security Division" (SSD) y en 1943 cambió por "Signal Security Service" (SSS). Hacia fines de 1943 pasó a denominarse "Signal Security Agency" (SSA) hasta 1945 cuando pasó a llamarse "Army Forces Security Agency" (AFSA). Por el memorándum del 24 de noviembre de 1952 que revisa la "National Security Council Intelligence Directive" se incorpora a la "National Security Agency" (NSA) como nuevo miembro de la Comunidad de Inteligencia de EEUU, la que concentra actividades de SIGINT que hasta ese entonces tenían otros organismos.

La cooperación angloamericana en materia de inteligencia de señales tuvo un importante antecedente en una operación realizada por el Reino Unido, mientras se encontraba en plena Primera Guerra Mundial. El 16 de enero de 1917 los servicios de inteligencia británicos interceptan un telegrama alemán encriptado, el cual es descifrado por la "Room 40". El documento era enviado por el ministro de Asuntos Exteriores del Imperio Alemán Arthur Zimmermann al embajador en México, Heinrich von Eckardt, donde se indicaba que debía proponer al gobierno mexicano una alianza para enfrentar a Estados Unidos a cambio de prestarle asistencia financiera y armamento, junto a la promesa de ayuda para la recuperación de los territorios de Texas, Nuevo México y Arizona, perdidos por el Tratado de Guadalupe-Hidalgo en 1848.

La alerta del Reino Unido sobre el contenido del "Telegrama Zimmermann", condujo a Estados Unidos a la inmediata ruptura de relaciones con Alemania y fue uno de los motivos que lo impulsó abandonar el aislacionismo e ingresar a la Primera Guerra Mundial, el 6 de abril de 1917.

Concluida la guerra, Reino Unido y EEUU no solo pusieron en su mira a países considerados oponentes, sino que también comenzaron a considerar al Movimiento Comunista Internacional dentro de sus objetivos, y así los servicios de inteligencia se dieron a la tarea de monitorear las comunicaciones de sus seguidores.

En la década del 20, la Inteligencia Naval de EEUU -OP-20-G junto con el FBI y la policía de Nueva York-, lograron apropiarse de los códigos del Consulado japonés

El Government Code and Cypher School (GC&CS) una instalación militar localizada en Buckinghamshire (Inglaterra) en la que se realizaron los trabajos de descifrado de códigos alemanes durante la Segunda Guerra Mundial. Recibe su nombre de la mansión victoriana que domina el enclave. La primera computadora Colossus fue diseñada y construida en Bletchley Park permitiendo romper los códigos de la máquina alemana Enigma.

El Government Code and Cypher School (GC&CS) en Bletchley Park (Reino Unido). Foto: Steve Montana Photography.

en Nueva York, que sirvió como base para muchas de las labores de criptoanálisis previas a la Segunda Guerra Mundial, aunque esto no fue suficiente para evitar el ataque a Pearl Harbor.

En ese período ambos países orientaron la inteligencia a sus áreas de especial interés geoestratégico. Estados Unidos trabajó en la interceptación de las comunicaciones de Japón. Especialmente a partir de la invasión de Manchuria en 1931, desarrollando una cadena de estaciones de escucha ubicadas en Hawai, Islas Aleutianas, Corregidor, Samoa, Guam, y Shanghai entre otras. A las que se sumaban unidades de superficie con capacidad de monitoreo de señales. El Reino Unido se dedicó al control de las comunicaciones de Alemania, Medio Oriente, la India. Y a partir de 1936, con el advenimiento de la Guerra Civil española, intensificó las operaciones sobre la Unión Soviética.

A principios de 1939 el servicio secreto británico instaló el Government Code and Cypher School (GC&CS) en Bletchley Park, que se convirtió en el centro de una enorme red de interceptación y captura de tráfico cifrado orientado principalmente a las comunicaciones del Eje. Su trascendencia se valoraría con la entrada del Reino Unido en la Segunda Guerra Mundial, luego de la invasión de Alemania a Polonia del 1 de septiembre de 1939.

El 31 de agosto de 1940[5] a propuesta de la Misión Militar de Estados Unidos en Londres fue celebrada una reunión, donde se establecieron las bases para un intercambio periódico de información entre ambos países en materia de inteligencia de señales. A principios de 1941, EEUU entregó al GC&CS una máquina "Purple", usada para desencriptar la correspondencia diplomática de Japón y más tarde empezó la colaboración en el ámbito criptoanalítico con la asignación de un oficial de enlace[6].

La captura del submarino alemán U-110, el 9 de mayo de 1941, permitió a los británicos apropiarse de una máquina de cifrado rotatorio Enigma[7], junto con el libro de códigos, manuales de señales y documentos encriptados. En junio de 1941, el GC&CS organiza el programa de criptoanálisis de la documentación alemana llamado "Ultra[8]" y con el auxilio de una máquina desencriptadora Magic descubre el funcionamiento de Enigma. La posibilidad de acceder a los códigos empleados por la flota alemana, daría a los británicos y estadounidenses una importante ventaja estratégica en la Guerra Naval.

Con el ataque de Japón a la flota norteamericana en Pearl Harbor el 7 de diciembre de 1941 y la declaración de guerra a Alemania e Italia el 11 de diciembre, EEUU entra en la Segunda Guerra Mundial. La Alianza militar angloamericana que se dio en todos los teatros de operaciones fortaleció las actividades de cooperación en inteligencia, y en 1942 grupos de criptoanalistas de ambos países trabajaban juntos en Bletchley Park.

El primer acuerdo que formaliza la especial relación de cooperación en inteligencia de señales entre los aliados, fue el Acuerdo Holden del 2 de octubre de 1942, realizado entre el U.S. Navy y el GC&CS, y será la base de sucesivos acuerdos[9].

En 1943 Canadá se suma a la labor de los Aliados, prestando asistencia en inteligencia de señales para el seguimiento de submarinos alemanes, y en su tarea los

La máquina Enigma que disponía de un mecanismo de cifrado rotatorio, que permitía usarla tanto para cifrar como para descifrar mensajes. Foto: Steve Montana Photography.

El telegrama Zimmermann. Foto: National Archives

tres países trabajan en tan estrecha colaboración, como si conformaran una organización única.

El 17 de mayo de 1943 se firma en Bletchley Park el Acuerdo BRUSA[10] , que establece la cooperación durante la guerra entre el US War Department (que involucra al SSA y OP-20-G) y el GC&CS. En este acuerdo regula el intercambio de información relativa a la localización, identificación e interceptación de señales, el descifrado de los códigos y claves. Así como el manejo conjunto y distribución del material secreto.

Se establece el reparto de áreas de responsabilidad, y según el criterio de división del esfuerzo en los diferentes teatros de operaciones. EEUU se encargaba principalmente de las comunicaciones de Japón, mientras que los británicos cubrían las comunicaciones alemanas e italianas. También se formaliza el intercambio de personal y tres unidades del SSA, fueron destacadas en Bletchley Park participando en tareas de colección, análisis y seguridad.

La gran confianza que generó el acuerdo, permitió a los británicos develar a sus nuevos socios el mayor secreto que habían mantenido oculto hasta entonces: los éxitos en la decodificación de señales alemanas logrados por "Ultra".

Inmediatamente después de finalizada la guerra en Europa, el Reino Unido buscó continuar con la Alianza, y miembros del servicio de inteligencia británico. Establecieron contactos con todos los participantes, concertando con Australia el aporte de personal y recursos técnicos a fin de apoyar el esfuerzo de EEUU en la guerra en el Pacífico. Para ese entonces la planta de personal de la alianza -entre civiles y militares- era de aproximadamente 40.000 miembros, donde la mitad era del Reino Unido.

Un importante antecedente a las actividades de control masivo de las comunicaciones se produce en agosto de 1945, cuando la AFSA pone en funciones el proyecto SHAMROCK que tenía por finalidad la captura y el control de todos los cables telegráficos que ingresaban o salían de EEUU. El programa fue continuado por la NSA hasta 1975, año en el que fue desactivado.

En septiembre de 1945, Truman firmó un memorándum secreto[11] por el que en consideración a la importante contribución de las unidades criptoanalíticas al éxito Aliado en la derrota del Eje, autoriza al Ejército y la Armada de EEUU a continuar la colaboración con los británicos en SIGINT, lo que permitió entablar negociaciones con el fin de establecer una Alianza para tiempo de paz.

El criterio británico era propiciar la integración en el consorcio de otros países del Commonwealth. Por ello una delegación británica estableció contactos con servicios de inteligencia de Canadá y de Australia para concertar su posible participación.

Entre febrero y marzo de 1946, se celebró una conferencia para revisar el Acuerdo BRUSA y negociar los detalles del nuevo acuerdo, donde se establecerían nuevas regulaciones de seguridad, procedimientos y protocolos para la cooperación en las actividades de inteligencia de señales. Entre varios temas tratados, el 5 de marzo de 1946[12] fue firmado el Acuerdo "British-US Communication Intelligence Agreement[13] " que establece el intercambio de información relacionado con operaciones de comunicaciones extranjeras en materia de colección de

tráfico, adquisición de comunicaciones y equipamiento, análisis de tráfico, criptoanálisis, descifrado y traducción, y adquisición de información respecto de organizaciones de comunicación, prácticas, procedimientos y equipamiento.

En los años sucesivos continuaron las negociaciones, concluyendo la redacción del texto final del acuerdo en las reuniones del 15 al 26 de Julio de 1948[14] . Posteriormente se incorporó como miembro a Canadá y más tarde, en 1956 se incluyó a Australia y Nueva Zelanda.

Durante la Guerra Fría se suscribieron convenios específicos con países que no formaban parte plena de la Alianza. Se establecieron relaciones de cooperación de limitado alcance. En un inicio se sumaron Noruega, Dinamarca, República Federal de Alemania y tiempo después se extendieron a Italia, Turquía, Holanda, Suecia, Singapur, Corea del Sur, Francia, España, Filipinas, Irlanda e Israel.

La comunidad de inteligencia de señales[15] quedó finalmente integrada por las siguientes agencias: la "US National Security Agency (NSA)", la "British Government Communications Headquarters (GCHQ)", la "Communications Security Establishment Canada (CSEC)", la "Australian Defence Signals Directorate (ASD)", y la "Government Communications Security Bureau (GCSB)" de Nueva Zelanda. Si bien a la Alianza se la conoce como "UKUSA", en forma coloquial se la denomina "Cinco Ojos" o "FVEY. James Cox[16] , explica que el nombre de "Cinco Ojos" surge de la clasificación de los documentos secretos que cuando se permitía el acceso de todos los participantes de la Alianza, el sello de clasificación dice: "SECRET—AUS/CAN/NZ/UK/US EYES ONLY", que está dirigido a los cinco miembros de la comunidad de inteligencia.

En la actualidad, UKUSA es la estructura de inteligencia de señales más importante del mundo y conforma una galaxia de medios de obtención y análisis en la que intervienen satélites militares y de uso civil, buques, submarinos, aviones y una inmensa red de computadoras terrestres, que junto a numerosas estaciones fijas de rastreo y escucha, pueden interceptar casi la totalidad del tráfico de comunicaciones, trasmitiéndolas en segundos a los centros de procesamiento.

A través de sus capacidades, se accede a todo tipo de comunicaciones electrónicas y señales[17] . Sean las transmitidas a través de satélite, cables submarinos, fibra óptica, internet, telefonía fija y celular, señales electromagnéticas o de radio de casi todo el mundo. Se le atribuye el acceso a miles de millones de comunicaciones por día, donde la captura, la clasificación y el análisis de las interceptaciones se realiza mayormente en forma automatizada.

Las principales bases de operaciones de UKUSA se encuentran en EEUU, en la central de NSA en Fort Meade y Utah Data Center; en el Reino Unido, el cuartel general del GCHQ (The Doughnut) de Cheltenham y en Menwith Hill; finalmente en Australia, en Pine Gap.

La cooperación en materia de personal no reconoce diferencia de países. Así, en Menwith Hill en el año 2014, de los 1800 empleados que se calculan trabajaban en la base, 400 eran británicos y 1200 norteamericanos de NSA.

En la gestión de inteligencia, además de analistas, trabajan diferentes tipos de especialistas tales como científicos en variadas disciplinas, lingüistas, matemáticos, físicos, criptógrafos y criptoanalistas, programadores y hackers, expertos en radiofrecuencias, operadores de puestos de escucha entre otras.

Para cumplir su cometido, UKUSA reparte su espacio de actuación ampliando los criterios establecidos en 1946, donde Estados Unidos, si bien tiene capacidad de control de gran parte del tráfico de comunicaciones de todos los países, centra su tarea en Asia, Rusia asiática, el norte de China, Latinoamérica y el Caribe, donde cuenta con estaciones en Puerto Rico, Brasilia, Bogotá, Caracas, Ciudad de México y Ciudad de Panamá[18] . Gran Bretaña [19] intercepta principalmente las comunicaciones en Europa, Rusia, África, aunque tiene instalaciones en todos los continentes. En América posee dos estaciones de escucha identificadas: Daniels Head en Bermuda y Mount Pleasant en las Islas Malvinas. Canadá cubre Centro y Sudamérica, Australia se dedica a las comunicaciones de Indochina, Indonesia y el sur de China, mientras que Nueva Zelanda tiene a su cargo el Pacífico occidental.

Dentro de la comunidad, Estados Unidos es el país que posee la mayor cantidad de medios, y su principal organización es la NSA, que coordina en materia de SIGINT a unas 17 agencias de inteligencia, conformando sistemas de gran complejidad. Así por ejemplo en la coordinación interagencial de las acciones del campo cibernético, están a cargo del United States Cyber Command[20] (USCYBERCOM) que funciona bajo el mando del Comando Estratégico de Estados Unidos (USSTRATCOM) y su comandante es el Director General de la NSA, que a su vez también es el jefe del Servicio Central de Seguridad (CSS).

La NSA es la más grande, secreta y probablemente la organización de inteligencia más cara de EEUU. Con estaciones de inteligencia, barcos, submarinos, aviones y satélites que actúan como plataformas de las operaciones de espionaje global, lo que le proporciona una inmensa capacidad de colección de inteligencia[21] . Su cuartel general se encuentra en Fort Meade, y su estructura concentra gran parte de los recursos técnicos de la alianza UKUSA. Cuenta con aproximadamente 50.000 empleados en los EEUU, (se calculan 280.000 empleados en el mundo). Contiene un presupuesto anual (2013) de unos 52.600 millones de dólares[22] .

Se le atribuye a la NSA la financiación y diseño de numerosos proyectos tecnológicos aplicados al espacio cibernético, entre ellos la red ARPANET (Advanced Research Projects Agency Network), concebida a principios de la década de los 60 como una red de comunicaciones seguras para uso militar, capaz de subsistir a un eventual ataque nuclear, y es el origen del actual INTERNET.

La NSA a través del "Foreign Affairs Directorate" (FAD), también establece relaciones con otros países aliados de utilidad para UKUSA. En el marco de acuerdos de "cooperación concentrada", aportando tecnología, intercambio de información y desarrollo de programas cibernéticos específicos. Un importante nexo de cooperación fuera de la alianza UKUSA, es el que mantiene con la Unidad 8200 (Yehida Shmoneh-Matayim) de las Fuerzas de Defensa de Israel, similar en lo operativo a la NSA y el GCHQ[23] .

La comunidad Ukusa durante la Guerra Fría

El inicio de la Guerra Fría impuso nuevos desafíos a la comunidad UKUSA, dado que la confrontación bipolar se esparció a diversos escenarios de todo el mundo, en los que las potencias buscaron imponer su influencia. En esta época floreció la carrera armamentista junto a la disuasión atómica, y es también el tiempo del inicio de una revolución tecnológica que alcanzará a todo el campo de la inteligencia de señales.

En el período que va desde 1950 hasta fines de la década de los 90, los estadounidenses trabajaron principalmente en operaciones de inteligencia electrónica y de señales sobre la Unión Soviética y de sus aliados en el mundo, cubriendo también a China, Vietnam, Corea del Norte, Centroamérica y Cuba, mientras el Reino Unido hacía lo propio especialmente en Medio Oriente, la India, África, Irlanda del Norte y parte del Pacifico. Canadá, Australia y Nueva Zelanda apoyaron las operaciones de sus aliados en diversos escenarios, como en el caso del área Asia-Pacífico a mediados de la década de los 50, donde tuvieron a su cargo el control de los grupos procomunistas de Malasia, y un poco más tarde en Tailandia e Indonesia. Durante el desarrollo de la Guerra de Corea entre 1950 y 1953, los 5 países miembros de la comunidad UKUSA participaron en la coalición auspiciada por las Naciones Unidas contra las Fuerzas norcoreanas y sus aliados, trabajando en operaciones de interceptación de las comunicaciones y señales de sus enemigos.

Al finalizar la guerra con la división definitiva del país, se mantuvo la tensión entre EEUU y Corea del Norte. La situación más grave entre ambos países se produjo en enero de 1968, cuando Corea del Norte capturó el barco USS PUEBLO (AGER-2) que cumplía misiones ELINT y SIGINT cerca del puerto de Wonsan y su tripulación fue apresada. Siendo liberados después de casi un año de difíciles negociaciones. Otro serio incidente ocurrió en abril de 1969, cuando un avión norteamericano de inteligencia de señales EC-121 cayó abatido por el fuego de un MIG-17 norcoreano, sobre el Mar del Japón.

A partir del lanzamiento del satélite soviético Sputnik [24] el 4 de octubre de 1957 y del estadounidense Explorer en febrero de 1958 se da inicio a una vertiginosa carrera de desarrollo de tecnología aeroespacial a la que se suman buscando su preeminencia el Reino Unido, China y Francia.

Estados Unidos inicia en 1959 sus programas satelitales SIGINT-ELINT con el proyecto CORONA y en 1960 con SAMOS, que en diferentes versiones poseían capacidades de reconocimiento visual y de comunicaciones. Más tarde se lanzan los satélites tipo FERRET, para interceptación del espacio radioeléctrico. En 1968 se inicia la serie CANYON, continuando con las series RHYOLITE, JUMPSEAT, AQUACADE. En la década de los 70 se incorporan los satélites tipo CHALET, KENNAN, VORTEX, MAGNUM, MERCURY y ORION. En los 90 se agrega la serie TRUMPET de intercepción de telefonía celular y frecuencias de radio.

En 1957 aparece el avión de reconocimiento Lockheed U-2, empleado también para SIGINT y ELINT. Los que participaron en numerosas misiones durante la Guerra Fría en particular sobre Cuba, la Unión Soviética, China y Vietnam. El U2 fue modernizado en sus diferentes versiones y por su calidad y prestaciones en la actualidad aún se encuentra en operaciones. La más conocida de las acciones en la que participó el U2 fue en la llamada "Crisis de los Misiles", cuando en el mes de oc-

tubre de 1962, la Unión Soviética inició la construcción de silos contenedores de vectores nucleares y fueron descubiertos a partir de fotografías obtenidas por estos aviones.

Durante el conflicto en Vietnam entre la década de los 60 y 70, los esfuerzos técnicos de UKUSA se concentraron en las operaciones sobre el sudeste asiático. Incorporando además como objetivos a Laos y Camboya.

La Guerra de Malvinas, fue un nuevo desafío para la comunidad UKUSA, donde los británicos además del empleo de los medios propios, contaron con la asistencia en todos los campos de la inteligencia de los restantes miembros de la alianza. Iniciada la guerra en abril de 1982, los británicos lanzaron la Operación Corporate a fin de reconquistarlas, y en su planeamiento una cuestión importante era establecer cuál sería el grado de ayuda que EEUU les proveería. El Acuerdo de 1946, comprometía a UKUSA a compartir inteligencia en las áreas de responsabilidad geográfica de cada uno y siendo que el conflicto se desarrollaba en el Atlántico Sur, -área de competencia de EEUU-, resultaba crítico para el Reino Unido que su socio proveyera todo el aporte de inteligencia disponible.

Sede de la NSA Fort Meade, la organización de inteligencia más grande de los Estados Unidos. Foto: AP Photo/Patrick Semansky

Entre las múltiples contribuciones de EEUU, se destaca la colaboración en SIGINT a través de los satélites de inteligencia de señales de reconocimiento y vigilancia de comunicaciones y meteorológicos, donde la avanzada tecnología de los sensores y los recursos de guerra electrónica constituyeron un apoyo decisivo para el desenlace de las operaciones militares.

El GCHQ contaba para sus operaciones de SIGINT y ELINT con los sistemas de satélites SKYNET y ZIRCON, a los que se sumaban medios: aéreos, navales y terrestres; junto a las estaciones de la Isla Ascensión, Belice, Australia, y Nueva Zelanda, entre otras, que proveían la información al cuartel general de Cheltenham.

La mayor limitación de los británicos en el uso de los satélites norteamericanos se debió a que la NSA los tenía orientados hacia sus blancos en el Hemisferio Norte. Así su empleo requirió una gran coordinación puesto que sólo podían ser reorientados hacia el Atlántico Sur por cortos periodos de tiempo, y por esta razón el GCHQ accedía a su uso solo por unas pocas horas al día.

La misión más importante que los británicos asignaron a los satélites norteamericanos VORTEX era la interceptación de las comunicaciones argentinas entre el Comando en Buenos Aires y las Fuerzas en las islas. Pero el requerimiento más urgente eran los partes de la salida de aviones de combate en dirección hacia las islas. Aunque esto se logró con relativo éxito, ya que las Fuerzas argentinas mantuvieron una estricta disciplina de silencio de radio, y aplicaron técnicas de cifrado, salto de frecuencia, escalonamiento del espectro, entre otras contramedidas.

También tuvieron el apoyo de los sistemas satelitales de reconocimiento y vigilancia KENNAN "KH-11". Capaces de proveer imágenes del rango visible con una resolución geométrica cercana a 0,15 metros y un área de cobertura variable según las necesidades operativas. Así como la posibilidad de la ubicación nocturna de blancos, por la generación de imágenes de alta resolución en infrarrojo. Esto permitió a los británicos contar con imágenes del dispositivo de Defensa argentino en las islas y la localización de las fuerzas, revelando en forma completa el orden de batalla aéreo, naval y terrestre[25]. Así como también blancos en territorio continental, tales como la posición de aeropuertos, unidades militares, bases navales y los lugares de probable almacenamiento de misiles Exocet.

Los documentos desclasificados por EEUU y el Reino Unido relativos a las relaciones entre ambos países durante la guerra, son explícitos en cuanto la colabora-

El barco USS Pueblo fue capturado en 1968 por embarcaciones coreanas cuando cumplka misiones en altamar. Foto Official U.S. Navy Photograph

ción y es elocuente el informe de la reunión[26] entre el Secretario de Estado Alexander Haig, con la Primer Ministro Margaret Thatcher, donde se encuentra el agradecimiento británico a la ayuda en materia de inteligencia. También es esclarecedor el artículo de John Lehman[27] -Secretario de la Armada de EEUU durante la guerra- en el que habla sobre el rol de su país en el conflicto de Malvinas, y del apoyo brindado a los británicos durante el conflicto.

Tecnología de Sigint para el control de comunicaciones a nivel mundial

Con el fin de controlar las comunicaciones militares de la Unión Soviética y sus aliados durante la Guerra Fría, la NSA desarrolló el programa ECHELON, que fue puesto en funcionamiento en la década del 70, y en 1981 se integraron al Sistema todos los países de la Alianza UKUSA. Su existencia fue develada a través de defectores y denuncias que tuvieron eco en los medios de comunicación. Principalmente por su vocación de espionaje en el campo de la inteligencia económica.

La primera noticia sobre la existencia de un programa de captura masiva de comunicaciones se produjo en 1972, cuando el agente de NSA Perry Fellwock reveló en un reportaje[28] información sobre su funcionamiento.

A mediados de 1988, Margaret Newsham[29] , contratista de la NSA para el desarrollo de software de SIGNT en Menwith Hill hace pública la existencia del programa ECHELON. El caso toma notoriedad por la revelación de Newsham sobre la interceptación de los teléfonos del Senador Strom Thurmond y otros políticos norteamericanos, manifestando que le perturbó saber que el programa en el que trabajaba no se dedicaba exclusivamente al espionaje de la Unión Soviética o de China. De sus revelaciones surgió que el programa tenía el nombre de código P415 que el software principal eran SILKWORTH y SIRE, y que para la interceptación de comunicaciones se usaban satélites VORTEX.

Poco tiempo después, en agosto de 1988, el periodista británico Duncan Campbell en un completo artículo[30] expuso detalles de ECHELON y de otros programas de SIGINT y de alta tecnología desarrollados en Menwith Hill, junto a sus socios de UKUSA.

Desde su creación ECHELON pasó por sucesivas actualizaciones en consonancia con los avances de la tecnología, y sus capacidades se orientaron a la interceptación mundial de todo tipo de comunicaciones telefónicas, fax, tráfico de datos, internet, señales de satélite y radio, internet, cables submarinos, y todo lo que pueda ser transmitido por vía de satélites, microondas, celular, fibra óptica o radio.

En el estudio realizado por Germán Pachón Ovalle [31] , -donde incursiona en aspectos técnicos de ECHELON-, explica que las señales capturadas por el sistema, se procesan en una serie de supercomputadoras llamadas "Diccionarios", los que en cada comunicación buscan e identifican patrones determinados (direcciones, palabras, frases o incluso voces específicas, etc.), lo que se evalúa automáticamente mediante filtros.

Cuando se detecta una comunicación que contiene alguna palabra clave o combinaciones de ellas, el sistema informático inicia el proceso de monitoreo y cap-

tura. Luego de su clasificación es enviada a los centros de análisis a donde se transcribe descifra, traduce e interpreta su contenido, guardándose como un informe. Finalmente se le asignará un código de identificación, perteneciente a la agencia a la que será remitido el informe. Lo que se hace a través de "Platform" -el sistema de interconexión de la red UKUSA- quedando la información para su uso.

El espionaje económico ha sido también tarea de ECHELON[32] y fue otro de los motivos que permitió la detección de la red, ya que varios países y empresas afectadas tuvieron a su cargo las investigaciones que determinaron su existencia.

El completo y revelador informe de Duncan Campbell al Parlamento Europeo titulado "Capacidades de Interceptación en 2000[33] ", expone sobre las actividades de inteligencia económica y el uso de información recolectada por la red ECHELON, con el fin de proporcionar ventajas comerciales a empresas de los países miembros de UKUSA.

En el documento se presenta el caso de la información comercial interceptada por la red en el año 1994, y que fue suministrada a la compañía estadounidense Raytheon para su beneficio. Ocasionando la pérdida de un contrato con Brasil de 1300 millones de dólares que estaba por lograr el grupo francés Thompson-CSF. Ese mismo año, la red proporcionó información esencial obtenida de las negociaciones secretas entre Arabia Saudita y la empresa Airbus Industrie, a favor de las estadounidenses Boeing y McDonnell Douglas, las que lograron un contrato de 6000 millones de dólares con el país árabe, en perjuicio de la empresa aeronáutica europea.

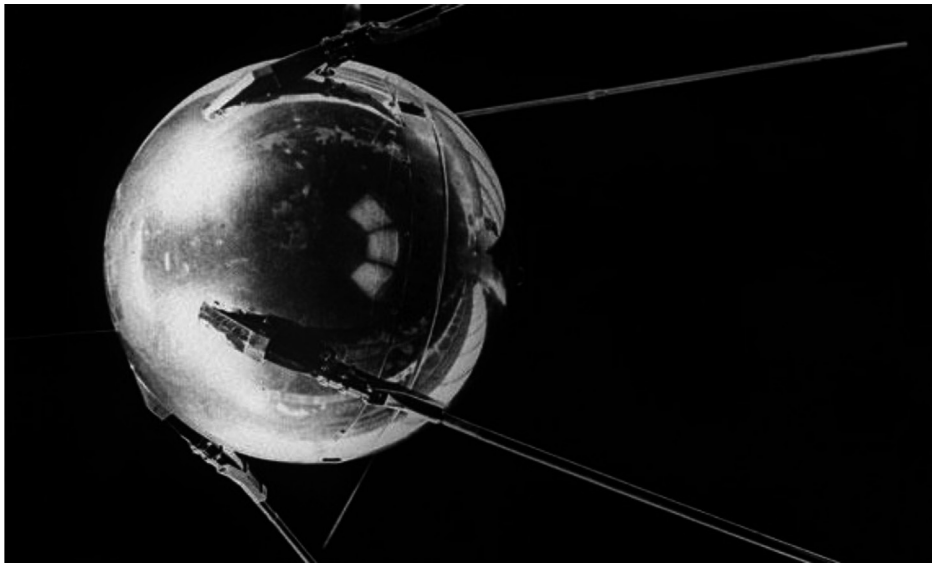
En función de los informes *"Una aproximación a las tecnologías de control político"*[34] y *"Capacidades de Interceptación en el 2000"*, junto a los numerosos reclamos de países e instituciones, el 5 de julio de 2000 el Parlamento Europeo creó una comisión para la investigación del tema. En el Reporte del Comité Investigador del 11 julio de 2001[35] y en el Acta del 5 de septiembre de 2001 [36], el Parlamento Europeo reconoce oficialmente la existencia y la naturaleza de ECHELON, al expresar que no hay ninguna razón para seguir dudando de la existencia de un sistema de interceptación de las comunicaciones a nivel mundial. Resultado de una cooperación entre los Estados Unidos, el Reino Unido, Canadá, Australia y Nueva Zelanda y que el fin del sistema es la interceptación como mínimo de comunicaciones privadas y comerciales, y no militares. Además se identifican al menos 28 casos en los que muestran la participación de la alianza UKUSA en actividades de inteligencia económica, que significaron millonarias pérdidas económicas a la industria europea.

El empleo de ECHELON para espionaje de comunicaciones diplomáticas, fue revelado en el año 2003 por Katharine Gun[37] , traductora del GCHQ que trabajaba en el Consejo de Seguridad de la UN, al difundir un informe secreto[38] .

El memorándum divulgado fue producido por el jefe de la Sección "Objetivos Regionales" de la NSA, Frank Koza, donde se refiere al espionaje realizado por la NSA y el GCHQ, sobre miembros de las delegaciones de Angola, Camerún, Chile, México, Guinea, y Pakistán[39] , al entonces Secretario General de la ONU Kofi Annan, y a otros objetivos vinculados a la organización internacional.

Nuevos programas con empleo masivo de tecnología

En el 2002 tomó conocimiento público el programa Trailblazer, a través de las denuncias de Kirk Wiebe, Wi-



El satélite soviético Sputnik 1, cuyo lanzamiento se produjo el 04 de octubre de 1957. Foto: Gerald Boerner.

lliam Binney, Ed Loomis de la NSA, y Diane Roark ante el Departamento del Inspector General de Defensa, por sospecha de delitos en su adquisición y por violación a la ley de inteligencia de EEUU. Trailblazer era una plataforma desarrollada para uso de la NSA por el consorcio de Boeing, Computer Sciences Corporation, y Booz Allen Hamilton, a un costo de 280 millones de dólares, y su misión era la captura y análisis masivo de redes de comunicaciones, internet, con capacidad para el control de telefonía celular y correos electrónicos.

Tiempo más tarde las denuncias de Thomas Drake[40] , Thomas Tamm, y Russ Tice, pusieron nuevamente en la prensa[41] la existencia de programas de espionaje masivo contra la población norteamericana por parte de la NSA. Ese mismo año, el hacker Samy Kamkar[42] denunció el seguimiento, control y colección ilícita de datos y comunicaciones de telefonía celular a nivel global a través de una plataforma que accede a teléfonos con sistema operativo Android (Google), iOS (Apple) y Microsoft Windows.

Pero el hecho de mayor gravedad en la historia de las denuncias sobre las actividades de inteligencia de UKUSA, se produjo el 5 de junio de 2013, cuando el contratista de NSA Edward Snowden comenzó a aportar información sobre miles de documentos secretos a los diarios The Guardian[43] y Der Spiegel[44] , relevando la existencia de una inmensa variedad de operaciones de SIGINT, a partir del establecimiento de programas de vigilancia y colección masiva de comunicaciones.

Tan grave era la información contenida en los documentos divulgados, que el 9 de junio el Director de Inteligencia Nacional de EEUU, James Clapper[45] reconoció el inmenso daño que las acciones de Snowden ocasionaban a las capacidades de inteligencia del país al exponer la información secreta y de igual manera David Omand, ex asesor de la inteligencia del Reino Unido, lo consideraba como una de las pérdidas más catastróficas sufrida por la inteligencia británica[46] .

Se calcula que la cantidad de documentos sustraídos por Snowden llegarían a 1.7 millones de archivos de EEUU[47] , 58.000 del Reino Unido[48] y 20.000 de Australia[49] , y muchos fueron entregados a los principales medios de comunicación mundiales, entre ellos a The Guardian, Der Spiegel, The New York Times, El País, The Washington Post, Le Monde, NRC, L'espresso, Canadian Broadcasting Corporation, O Globo, y Australian Broadcasting Corporation.

Así a partir de los documentos difundidos por Snowden, quedó expuesta la mayor red mundial de inteligencia de señales[50] , develando un programa estructural de colección y análisis de información, organizado por la comunidad UKUSA. Basado en inmensos recursos tecnológicos, con masivas escuchas y grabaciones telefónicas, vigilancia exhaustiva de correos electrónicos, análisis de usuarios, perfiles y actividades en las redes sociales, con rastreo de información en tiempo real, y la participación de las grandes empresas del sector de las comunicaciones e informática.

GCHQ (The Doughnut) en Cheltenham es la sede Gubernamental de Comunicaciones británica

El amplio conjunto de herramientas automatizadas de inteligencia cibernética, se basan en variados recursos de hardware, plataformas, programas informáticos, implantes y toda clase de instrumentos técnicos de utilidad para actividades de captura masiva o para operaciones "a medida". Su diseño permite la obtención y colección de datos, y con el empleo de motores de búsqueda y analizadores, que junto a diferentes programas que actúan a través de capas, donde la información obtenida es tamizada, clasificada y ordenada por relevancia, para su posterior análisis.

La dimensión de las comunicaciones telefónicas intervenidas surge de un informe donde se establece que entre finales de 2012 y comienzos de 2013 se habrían espiado más de 200 millones, de las cuales 70,3 millo-

de criptografía e inteligencia. Foto: Steve Montana Photography.

nes corresponden a Francia, 46 millones de Italia y 60 millones de España. En operaciones "a medida", se han intervenido las comunicaciones de líderes políticos del mundo[51] , entre los que se cuentan Dilma Rousseff, Angela Merkel, Mariano Rajoy, François Hollande y Enrique Peña Nieto.

Algunos de los numerosos recursos de inteligencia cibernética desarrollados por UKUSA son los siguientes:

PRISM (US-984XN)[52] : Su nombre proviene de la sigla de "Planning Tool for Resource, Integration, Synchronization, and Management" y es una plataforma que posee un conjunto de herramientas desarrolladas por NSA.

Accede a todo el tráfico de internet y comunicaciones telefónicas, con capacidad de captura de correos electrónicos, vídeos, chat de voz, fotos, direcciones IP, notificaciones de inicio de sesión, transferencias de archivos y detalles sobre perfiles en redes sociales. Usando poderosas computadoras pueden decodificar, desencriptar, almacenar y analizar toda esa información casi instantáneamente.

Colaboran las empresas de servicios por internet como Microsoft, Yahoo, Google, Facebook, AOL, Skype, YouTube, Apple, entre otras. Dependiendo del proveedor, pueden recibir notificaciones en tiempo real cuando el blanco inicia una sesión o envía un email, o es posible monitorear mensajes de texto, voz o chat de voz.

La plataforma trabaja con aplicaciones que filtran la información capturada a través de un procesamiento por capas, donde participan: PRINTAURA que automatiza el flujo del tráfico. SCISSORS y PROTOCOL EXPLOITATION separan la información según sus características, ordenándola para su análisis. Las bases de datos y los análisis específicos se hacen con: NUCLEON (voz), PINWALE (vídeo), MINWAY (registro de llamadas) y MARINA (registros de Internet). En la capa final de filtrado están FALLOUT y CONVEYANCE que sirven para reducir la cantidad de información.

El analista accede a la información a través de la aplicación de consulta llamada UTT o Herramienta Unificada de Objetivos, donde al usuario le basta indicar un "área geográfica" y su "relevancia" para acceder a la información. Por ejemplo, si es diplomático, político, o puede identificar el blanco por su correo electrónico, perfil de Facebook, entre otras muchas vías de acceso.

TEMPORA[53] : Es una plataforma británica compartida con la NSA, diseñada para interceptación de comunicaciones de todo tipo mediante el acceso a redes informáticas y telefónicas y los datos de localización. Actúa sobre los cables de fibra óptica por donde circula gran parte de las comunicaciones telefónicas, internet y datos mundiales. El espionaje británico intercepta los cables provenientes de diversas regiones y desvía el tráfico a sus servidores, contando con la colaboración de las grandes empresas de telefonía del país, como la Telefónica O2, British Telecommunications o Vodafone.

UPSTREAM (ROOM641A)[54] : Es una plataforma alternativa a PRISM, similar a TEMPORA, que es utilizada por NSA para colectar gran parte del tráfico mundial de comunicaciones que circula a través de redes de cables de fibra óptica. En la operación, se vinculan herramientas[55] llamadas BLARNEY, FAIRVIEW, OAKSTAR y STORMBREW que apoyan la tarea de colección y procesamiento masivo de información. Cuenta con la colaboración de las empresas de telefonía AT&T, Verizon y BellSouth, entre otras

XKEYSCORE (XKS)[56] : Es una plataforma basada en un conjunto de aplicaciones informáticas y de hardware desarrolladas por NSA, para la obtención de información a través del tráfico de internet y de telefonía celular. Extrae y clasifica información de correo electrónico, mensajería de texto, páginas web, historiales de

navegadores y conversaciones digitales de usuarios. Puede analizar contenidos y metadatos y permite investigar por nombre, número de teléfono, dirección IP o por el idioma del usuario en Internet. Se accede a través de un gran cluster con cerca de 700 servidores y puntos de acceso distribuidos en bases y embajadas alrededor del mundo, donde el analista en la sesión de consulta accede con sencillez a una gigantesca base de datos y puede obtener información del blanco en tiempo real.

DISHFIRE[57] : Es un programa de colección y análisis empleado por UKUSA para la interceptación del tráfico mundial de telefonía celular. Posee capacidades de supervisión, captura, y colección de alrededor de 200 millones de mensajes de texto diarios[58] alrededor del mundo, obtenida por el acceso a redes de telefonía celular. La herramienta de análisis se denomina "PREFER", y procesa los mensajes de SMS extrayendo la información que contienen. Permite obtener los contactos y establecer ubicación del teléfono celular por sus capacidades de geolocalización a partir de las alertas de roaming. Puede determinar cambios de ubicación geográficos.

MUSCULAR (DS-200B)[59] : Es un programa desarrollado por el Reino Unido, que comparte con la NSA, que intercepta los cables que vinculan los centros de datos de Google, Yahoo o Hotmail[60] , para acceder a la información de los correos electrónicos u otras prestaciones .

BOUNDLESS INFORMANT[61] : Es una herramienta desarrollada por la NSA que le permite obtener estadísticas en tiempo real, para establecer el alcance concreto de su espionaje en cada país. Entre la información se destaca que a lo largo del mes de febrero de 2013, la agencia recopiló 3.000 millones de datos relacionados con ciudadanos estadounidenses.

TRACFIN[62] : Es un programa de colección de información bancaria y financiera usado por NSA. Analiza las transacciones de usuarios de grandes compañías de tarjetas de crédito, conformando una gran base de datos, especialmente orientada a operaciones de áreas designadas como geográficamente prioritarias. TRACFIN obtiene información bancaria accediendo a la base de datos de la organización llamada "Society for Worldwide Interbank Financial Telecommunication" (SWIFT), con sede en Bruselas, la que concentra las millones de transacciones bancarias que anualmente se realizan en el mundo.

BULLRUN y EDGEHILL[63] : Son aplicaciones desarrolladas por NSA y GCHQ, que se emplean como en forma accesoria a otras plataformas y sirven para eludir el cifrado online, lo que permite vulnerar los sistemas de encriptado y protocolos seguros conocidos como HTTPS. También tienen capacidad de utilizar la llamada "fuerza bruta", procedimiento aleatorio que permite analizar cada clave hasta encontrar la llave correcta. Esto hace vulnerable la codificación que protege los sistemas bancarios, el comercio global, así como permite acceder a múltiples datos sensibles, como los secretos comerciales o registros médicos.

Otros recursos de Ukusa para la captura de información

Se suman a la captura masiva de transmisiones en todo el espectro electromagnético e internet los recursos técnicos de hardware especial, ya sea a través de dispositivos de implante en equipos de comunicaciones, computadoras y cables, uso de antenas especializadas, entre muchos medios disponibles.

A requerimiento de la NSA, muchas empresas de la industria electrónica, fabricantes de hardware, insumos electrónicos y microprocesadores (Intel, AMD, entre otras), han incorporado ciertas características incluidas en la arquitectura de sus equipos y microprocesadores, que permiten el acceso a toda la información de los usuarios. Esto permite la captura de información a partir de los microprocesadores instalados en computadoras industriales y personales, teléfonos celulares, routers y otros dispositivos electrónicos.

Los microprocesadores empleados por la mayoría de los smartphones[64] poseen un procesador físico secundario adicional, que permite controlar en forma remota toda la información del aparato, tal como si fuera el usuario; accediendo a su ubicación, contactos, archivos, tráfico de ingreso o egreso. Pudiéndose grabar o activar la cámara, el micrófono, e incluso con la posibilidad de bloquear o apagar el aparato. Por ello, los smartphones son un objetivo prioritario por su amplísima capacidad de proporcionar información relevante.

Otro recurso proviene de la facilitación por parte de las empresas informáticas fabricantes de sistemas operativos o software, de la tecnología de cifrado empleada en esos programas. Esto permite ingresar a la información a través de las llamadas "puertas traseras" y acceder libremente a las computadoras u obtener la contraseña del usuario.

Según las revelaciones de Snowden, la NSA y sus socios reciben la cooperación de las empresas de software y de aplicaciones de internet[65] como Google, Microsoft, Facebook, Apple, entre otras, las que permiten acceder a las bases de datos e información personal de los clientes.

Microsoft está vinculada con un área de la NSA, que trabaja en la instalación de líneas de código secretos en sus productos e indica a los desarrolladores de programas qué agujeros de seguridad deben crear para que se pueda acceder a través de ellos. Estos agujeros de seguridad se encuentran en productos y servicios como Windows e Internet Explorer, Skype, SkyDrive, Outlook, entre muchos otros.

Otra de las muchas empresas privadas que colaboran con la NSA es NARUS, compañía estadounidense que pertenece a desde el 2010 a Boeing, y produce sistemas de vigilancia masiva. Entre las herramientas de inteligencia cibernética desarrolladas se encuentra NarusInsight, empleado para realizar vigilancia masiva y monitorización de las comunicaciones de internet en tiempo real, o el analizador de tráfico STA 6400.

Ciberoperaciones ofensivas

Diversas operaciones ofensivas han tenido como medio el uso de malware o software malicioso (virus, gusanos, troyanos, rootkits, scareware, spyware, adware intrusivo, etc.) e inclusive "cracking", herramientas útiles para infiltrarse, capturar datos, dañar computadoras o sistemas de información, y afectar gravemente infraestructuras críticas y redes de empresas de comunicaciones.

Según las revelaciones de Snowden a Der Spiegel y The Guardian, se atribuye a la NSA e Israel el desarrollo de Stuxnet, primer gusano informático para realizar sabotaje y destrucción de infraestructuras críticas, que tuvo como objetivo afectar el programa nuclear iraní.

Este gusano informático[66] fue descubierto en junio de 2010, luego de afectar a miles de computadoras del mundo. Su característica principal es que realiza la reprogramación de los sistemas SCADA, usados para el control y monitorización de procesos industriales, lo que altera el funcionamiento físico de las maquinarias[67] y por ello tiene capacidad de perturbar gravemente las infraestructuras críticas[68] .

El Stuxnet logró infectar el software de centros industriales iraníes, incluidos una planta de enriquecimiento de uranio, donde buscó alterar la velocidad de los rotores de las usinas, mientras que en forma simultánea evitaba que el sistema supervisor detectara anormalidades en el funcionamiento. De este modo cuando se identifica el problema el daño ya había sido causado. Su detección a evitó graves perjuicios, pero esta circunstancia retrasó la puesta en marcha de la planta nuclear de Bushehr.

Es también probable la participación de la NSA en la creación de malware como DuQu, Flame y Gauss, desarrollados para la obtención de información sensible sobre infraestructuras críticas para su posterior ataque. Según el reporte de incidentes realizado por Kaspersky Lab[69] , los países con mayor cantidad de ocurrencias verificadas por acción de estos malware fueron Irán, Sudan, Arabia Saudita, Siria, Líbano, Israel, y en menor grado Turquía, Iraq, Jordania y Egipto.

Entre las operaciones ofensivas denominadas "a medida"[70] , incluyen una amplia gama de intrusiones y ataques contra blancos precisos. Entre ellos instituciones, políticos y gobernantes del mundo, servicios de inteligencia de diversos países y operadores de telecomunicaciones. Empleándose recursos de piratería y el uso de software malicioso[71] .

Estación de escucha de la NSA en Bad Aibling (Alemania). Foto: AFP Photo / Christof Striache.

Protestas en los Estados Unidos en contra del espionaje cibernético. Foto: Mandel Ngan.

Reflexiones finales

1. La historia de la alianza UKUSA, muestra que es posible conformar una sólida estructura de inteligencia multinacional, cuando hay decisión política, comunidad de intereses y confianza entre los participantes. A pesar que cada organización miembro se guía por lo establecido por sus normas nacionales y se sustenta en los valores e intereses de su propio país, en la tarea técnica todos actúan de consumo en beneficio de la alianza, sustentados en una sólida lealtad y respeto profesional.

2. El sostenido crecimiento de la tecnología ha generado importantes capacidades en materia de SIGINT. Automatizando los procesos de búsqueda y obtención de la información. Actualmente casi todos los países disponen de la tecnología SIGINT y de inteligencia cibernética que les permite acceder a todo tipo de comunicaciones e internet, normalmente limitado a los posibles oponentes o al campo doméstico, y son muy pocos los países que han desarrollado programas de interceptación a las comunicaciones mundiales.

3. Se desconoce cuál es el provecho de los procedimientos de captura masiva de información a nivel mundial, ya que es obvio que la mayor parte de lo obtenido es inútil, irrelevante e inconsistente. Para alcanzar una universalidad de objetivos, el grado de sobrecarga informativa es inmenso, lo que hace escasa la posibilidad que del maremágnum informativo se rescate demasiado material útil como insumo de inteligencia. Esto implica un enorme dispendio en personal, medios y dinero, así como una innecesaria exposición a la contrainteligencia de los países y la acción de particulares como hackers o empresas que pueden develar dichas acciones, y en esto, las consecuencias del fracaso son proporcionales a la magnitud del objetivo.

4. No se ha podido dilucidar con claridad, cuáles son los objetivos perseguidos por la comunidad UKUSA, para justificar el masivo control de las comunicaciones mundiales sobre blancos mayoritariamente civiles. La intromisión arbitraria a la intimidad de los ciudadanos, es una grave violación legal que afecta la privacidad de los particulares, protegida jurídicamente en todos los países. Es igualmente grave que la comunidad de inteligencia haya llegado al extremo de operar dentro de sus propios países, aún en contra de las leyes que regulan su actividad. Curiosamente, la mayor derrota de la comunidad UKUSA no ha provenido del campo militar, sino ha sido consecuencia de sus acciones en el ámbito civil, las que quedaron expuestas públicamente en los medios de comunicación por parte de defectores y particulares afectados.

5. El caso de los defectores, muestra una gravísima falla en el personal de inteligencia en cuanto la falta de ética profesional, lealtad y compromiso hacia su país y a la estructura a la que pertenecen. Si bien una razón puede ser por el empleo intensivo de contratistas externos, sin identificación suficiente con la organización y sus valores. También es atribuible a errores en la selección del personal y a que la masividad en las necesidades de recursos humanos para sostener el gigantesco sistema, impiden una cuidadosa elección.

6. En el caso Snowden se evidencia la falta de compartimentación de la información, y es inverosímil que en la mayor organización de inteligencia del mundo, un analista haya podido acceder a la gigantesca cantidad de material altamente secreto. Peor

aún, que haya logrado copiar, reproducir o robar sin control miles de documentos, informes y cables ultra secretos, y ser difundidos libremente a la prensa mundial; lo que además de la posibilidad de trasgresión de todas las medidas de seguridad y protección de la información, indica la carencia de una contrainteligencia eficaz.

7. La exposición de las actividades de UKUSA al publico mundial, ha producido el deterioro de la confianza en países de su tradicional amistad y cercanía ideológica. En la medida que al ser convertidos en blancos de la inteligencia los ha puesto en la categoría de posibles adversarios -presentes o futuros- de esos países. Como contrapartida, la difusión de las actividades de inteligencia ha permitido a sus reales antagonistas contar con la información necesaria para articular las contramedidas adecuadas.

8. La inteligencia llevada a cabo en el campo económico por la comunidad UKUSA, pone en crisis el concepto intrínseco del liberalismo sostenido como dogma en esos países. El empleo de las herramientas de control y vigilancia para proveer información a sus empresas connacionales -e incidir en el mundo de la industria y el comercio-, desvirtúan su finalidad y contradicen los valores que proclaman esos países sobre el libre mercado, ya que se convierten en un mecanismo insidioso y desleal de intervención estatal en el mercado.

9. Todo plan es bueno hasta que se descubre y en este caso las derivaciones de la pérdida del secreto de los programas han tenido gravísimas consecuencias políticas, militares, tecnológicas y un superlativo perjuicio económico ocasionado por los billones de dólares invertidos que se han perdido.

Finalmente, analizando la problemática desde la óptica de la Defensa Nacional, el panorama planteado permite las siguientes reflexiones:

1. Es evidente la inmensa fragilidad de la seguridad en las tecnologías de información y comunicación de todos los países, donde frente a la descomunal cantidad de recursos SIGINT para vulnerarla, pareciera no existir seguridad absoluta en ese ámbito.

2. Como cualquier actividad de espionaje es una situación de conmoción a la seguridad nacional que debería ser seriamente considerada. Se trata de la injerencia de un conjunto de Estados en los asuntos de otros, poniendo en riesgo potencial la soberanía política, militar, industrial, científica y tecnológica de los países afectados. Esto ocasiona una grave perturbación a la seguridad en su conjunto, con consecuencias en el resguardo de las infraestructuras críticas y comunicaciones vitales.

3. Para hacer frente a las acciones del espionaje cibernético de las dimensiones analizadas, las contramedidas son complejas y requieren de la implementación de sólidas acciones en el campo de la seguridad de la información y de la seguridad informática. Esto impone la realización de una profunda revisión sobre aspectos políticos, estratégicos y de cultura institucional, determinando las vulnerabilidades y las capacidades, para así desarrollar todos los medios necesarios para enfrentar la amenaza.

La canciller alemana Angela Merkel junto al presidente estadounidense Barack Obama. Foto: Peter Schwarz.

REFERENCIAS

BIBLIOGRAFÍA

Aid, Matthew y Wiebes, Cees,"Secrets of Signals Intelligence During the Cold War and Beyond", Taylor & Francis, 2001.

Aldrich, Richard, "GCHQ", Harper Press, 2010.

Alvarez, David, "Allied and Axis Signals Intelligence in World War II" Portland, Frank Cass, 1999 pages 206-228

Andrew, Christopher, "The making of the Anglo-American SIGINT Alliance", en "In the Name of Intelligence: Essays in Honor of Walter Pforzheimer", NIBC Press, 1994

Hinsley, Harry, et al, "British Intelligence in the Second World War", Vol.I, Stationery Office Books, 1979, pág. 312 y ss.

Andrew, Christopher, "The making of the Anglo-American SIGINT Alliance", en "In the Name of Intelligence: Essays in Honor of Walter Pforzheimer", NIBC Press, 1994, pág. 100

Cox, James, "Canada and the Five Eyes Intelligence Community", Strategic Studies Working Group Papers, Canadian Defence & Foreign Affairs Institute and Canadian International Council, December 2012

Freeman, Peter, "MI1(b) and the origins of British diplomatic cryptanalysis" Intelligence and National Security, Volume 22, Issue 2, 2007 pág. 206-228

Ferris, John, "Before 'room 40': The British Empire and signals intelligence, 1898–1914", Journal of Strategic Studies, Volume 12, 1989 pág. 431-457.

Ferris, John, "The British army and signals intelligence in the field during the first World War" Intelligence and National Security, Volume 3, Issue 4, 1988 pág. 23-48

Erskine, Ralph, "The Holden agreement on naval Sigint: The first BRUSA?", Intelligence and National Security, Volume 14, Issue 2, 1999, pág. 187-197

Hager,Nicky, "Secret Power: New Zealand's role in the international spy network", Craig Potton Publishing, New Zealand, 1996

Hinsley, Harry, et al, "British Intelligence in the Second World War", Vol.I, Stationery Office Books, 1979

Johnson, Loch, "Strategic Intelligence", Praeger Security international, Volume 1,2,3,4 y 5, 2007

Lee, Bartholomew, "Radio Spies-Episodies in the ether wars", Antique Wireless Association Review, 2002.

Lehman, John, "Reflections on the Special Relationship", Naval History Magazine, Volume 26, Number 5- October 2012.

Parlamento Europeo "Desarrollo de la tecnología de vigilancia y riesgos del uso indebido de la información económica", Dirección General de Estudios, Dirección A, Programa STOA, Documento de trabajo para el Panel STOA, PE 168. 184 Vol. 2/5, Luxemburgo, octubre de 1999.

Parlamento Europeo "Una aproximación a las tecnologías de control político" Comisión de Libertades Públicas y Asuntos de Interior del Parlamento Europeo, enero de 1998. .

Parlamento Europeo "Report on the existence of a global system for the interception of private and comercial communications (ECHELON interception system) (2001/2098(INI)", Temporary Committee on the ECHELON Interception System, A5-0264/2001 PAR1

Parlamento Europeo, "Resolución del Parlamento Europeo sobre la existencia de un sistema mundial de interceptación de comunicaciones", Acta del 05/09/2001, ECHELON A5-0264/2001

Sánchez Medero, Gema, "Ciberterrorismo: la guerra del siglo XXI", El Viejo Topo, número 242, marzo de 2008, pág. 15-24.

Smith, Bradley, "The ultra-magic deals and the most secret special relationship, 1940-1946", Presidio, 1993

Richelson, Jeffery, "A Century of Spies: Intelligence in the Twentieth Century", Oxford University Press, 1997

Rodríguez Pérez, Carlos, "Tecnologías de vigilancia e investigación: El caso Echelon". Informe: Tecnologías de vigilancia e investigación, posgrado conocimiento, ciencia y ciudadanía en la sociedad de la información. Universitat de Barcelona, 2008

Thomas, Timothy, "Las estrategias electrónicas de China", Military Review, julio-agosto de 2001, pág. 72-79.

Urban, Mark, "UK Eyes Alpha: Inside Story of British Intelligence" Faber & Faber, 1996

West, Nigel, "The SIGINT Secrets: The Signals Intelligence War, 1900 to Today: Including the Persecution of Gordon Welchman". New York,W. Morrow, 1988

NOTAS

1 Tripodi, Hoja de vida de José Gabriel Paz, .

2 Ferris, John, "Before 'room 40': The British Empire and signals intelligence, 1898–1914", Journal of Strategic Studies, Volume 12, Issue 4, 1989, pág. 431 y ss.

3 Freeman, Peter, "MI1(b) and the origins of British diplomatic cryptanalysis" Intelligence and National Security, Volume 22, Issue 2, 2007 pages 206-228

4 Aldrich,Richard, "GCHQ", Harper Press, 2010, pag.13

5 Hinsley, Harry, et al, "British Intelligence in the Second World War", Vol.I, Stationery Office Books, 1979, pág. 312 y ss.

6 Andrew, Christopher, "The making of the Anglo-American SIGINT Alliance", en "In the Name of Intelligence: Essays in Honor of Walter Pforzheimer", NIBC Press, 1994, pág. 100

7 "Breaking Germany's Enigma Code", Andrew Lycet, en BBC, 17 de febrero de 2011. Ver en: http://goo.gl/0bkoN (Consultado el 13-10-2014)

8 Smith, Bradley, "Sharing Ultra in World War II", International Journal of Intelligence and Counterintelligence 2, no. 1 (Spring 1988), pág. 59-72

9 Se destacan como acuerdos derivados (extended agreements) el "BRUSA Agreement" del 14 de enero de 1944, y los acuerdos "Agreement between G.C.&C.S. and Negat (OP-20-G) on Japanese Naval Cryptanalytic Tasks" del 23 de Octubre de 1944, y "Proposals Made to OP-20-G on 4th June 1945 for British Sigint Effort on S.E.A.C. (Mountbatten's South EastAsia Command)" entre otros varios.

10 "Agreement between British Government Code and Cipher, School and U.S.War Department". Ver en http://goo.gl/TZqrJM (Consultado el 13-10-2014)

11 Smith, Bradley, "The ultra-magic deals and the most secret special relationship, 1940-1946", Presidio, 1993, pág. 211

12 "Not so secret: deal at the heart of UK-US intelligence", Richard Norton-Taylor en The Guardian, 25 de junio de 2010. Ver en http://goo.gl/lPdQao (Consultado el 13-10-2014)

13 "British-US Communication Intelligence Agreement". Ver en http://goo.gl/OyCtsI (Consultado el 13-10-2014)

14 "Communication Intelligence Agreement". Ver en http://goo.gl/r45R0x (Consultado el 13-10-2014)

15 "Newly released GCHQ files: UKUSA Agreement", The National Archives (archivos desclasificados del Reino Unido). Ver en http://goo.gl/2UYKqM (Consultado el 13-10-2014)

16 Cox, James, "Canada and the Five Eyes Intelligence Community", Strategic Studies Working Group Papers, Canadian Defence & Foreign Affairs Institute and Canadian International Council, December 2012

17 Martín de Santos, Inés y Martín Vega, Arturo, "Las fuentes abiertas de información. Un sistema de competencia perfecta", Inteligencia y Seguridad: Revista de análisis y prospectiva N° 8, Plaza y Valdés, Madrid, Junio-Noviembre de2010, pág. 105

18 "Puerto Rico como centro de espionaje para la CIA", Metro, 12 de julio de 2013. Ver en: http://goo.gl/YKqYJW (Consultado el 13-10-2014)

19 Aldrich,Richard, "GCHQ", Maps - Overseas British Sigint Stations Harper Press, 2010, pag.xiv

20 U.S. Department of Defense, Cyber Command, Fact Sheet, 21 May 2010 http://goo.gl/Q9qEub (Consultado el 13-10-2014)

21 Hager,Nicky, "Secret Power: New Zealand's role in the international spy network", Craig Potton Publishing, New Zealand, 1996, pag.21. El libro puede obtenerse en http://goo.gl/8mRVWC (Consultado el 13-10-2014)

22 "Black budget' summary details U.S. spy network's successes, failures and objectives", Gellman, Barton y Miller,Greg en The Washington Post, 29 de Agosto de 2013. Ver en: http://wapo.st/17mcAxu (Consultado el 13-10-2014)

23 "Inteligencia militar impulsa la alta tecnología", transcripción del artículo de Matthew Kalman en The Guardian del 12 de agosto de 2013, Embajada de Israel en Costa Rica – Red Diplomática de Israel. Ver en: http://goo.gl/ysDEiN (Consultado el 13-10-2014)

24 Desde el Sputnik hasta el año 2014, cerca de 7000 satélites fueron lanzados en el mundo con diferentes propósitos.

25 The National Security Archive, "Secretary's Military Forces,Argentina", Ver en: http://goo.gl/mwu3Yg (Consultado el 13-10-2014)

26 The National Security Archive, "Secretary's Meeting with Prime Minister Thatcher April 8: Falkland Islands Crisis" Pág. 3, punto 5. Ver en: http://goo.gl/n4hBBN (Consultado el 13-10-2014)

REFERENCIAS

27 Lehman, John, "Reflections on the Special Relationship", Naval History Magazine, Volume 26, Number 5- October 2012. Ver en http://goo.gl/30qw31 (Consultado el 13-10-2014)

28 "U.S. Electronic Espionage: A Memoir", Ramparts, Vol. 11, No. 2, Agosto 1972, pág. 35-50 (Perry Fellwock usa en el reportaje el seudónimo Winslow Peck)

29 "Suit Says Firm Misused Funds for Defense Job" articulo de Dan Morain en The Angeles Time, 07 de Julio de 1988, Ver en: http://goo.gl/12lYAa (Consultado el 13-10-2014)

30 "Somebody's Listening", articulo de Duncan, Campbell, en New Statesman Society, 12 de agosto de 1988, pág. 10-12. Ver en: http://goo.gl/7F6Gxh (Consultado el 13-10-2014)

31 Pachón Ovalle, Germán, "La red Echelon: Privacidad, Libertad y Criptografía", Programa de Doctorado en SIC, Universidad Oberta de Cataluña, Barcelona, 2004

32 Johnson, Loch, "Strategic Intelligence", Global Economic Espionage, The intelligence cycle: The flow of secret Information from overseas to the hightestcouncils of goverment, Praeger Security international, Volume 2, 2007, pág. 181 y ss.

33 "Desarrollo de la tecnología de vigilancia y riesgos del uso indebido de la información económica", Parlamento Europeo, Dirección General de Estudios, Dirección A, Programa STOA, Documento de trabajo para el Panel STOA, PE 168. 184 Vol. 2/5, Luxemburgo, octubre de 1999

34 El informe "Una aproximación a las tecnologías de control político" fue presentado en la Comisión de Libertades Públicas y Asuntos de Interior del Parlamento Europeo en enero de 1998, y fue realizado por la Fundación Omega de Manchester

35 "Report on the existence of a global system for the interception of private and comercial communications (ECHELON interception system) (2001/2098(INI)", Parlamento Europeo, Temporary Committee on the ECHELON Interception System, A5-0264/2001 PAR1

36 "Resolución del Parlamento Europeo sobre la existencia de un sistema mundial de interceptación de comunicaciones", Parlamento Europeo, Acta del 05/09/2001, ECHELON A5-0264/2001

37 "Interview: Whistleblower Katharine Gun", BBC News Online political staff at the TUC in Brighton, 15 de Septiembre de 2004. Ver en http://goo.gl/BvmfKS (Consultado el 13-10-2014)

38 "Revealed: US dirty tricks to win vote on Iraq war" The Observer, 2 Marzo de 2003. Ver en http://goo.gl/aeQ2mE (Consultado el 13-10-2014)

39 "Leaked memo suggests US manipulating UN" Australian Broadcasting Corporation Broadcast, 6 de Marzo de 2003. Ver en http://goo.gl/2A9Ywd (Consultado el 13-10-2014)

40 "Former N.S.A. Official Is Charged in Leaks Case", Scott Shane en New York Times, 15 de abril de 2010. Ver en http://goo.gl/SGCcD0 (Consultado el 13-10-2014)

41 "The Secret Sharer. Is Thomas Drake an enemy of the state?" por Jane Mayer, The New Yorker, 23 de mayo de 2011. Ver en http://goo.gl/5zKoPj (Consultado el 13-10-2014)

42 "What They Know Apple, Google Collect User Data" Angwin, Julia y Valentino-DeVries, Jennifer en The Wall Street Journal, 22 de Abril de 2011. Ver en http://goo.gl/e3neAu (Consultado el 13-10-2014)

43 "Edward Snowden, NSA files source: 'If they want to get you, in time they will'" Glenn Greenwald, Ewen MacAskill y Laura Poitras en The Guardian, 9 de junio de 2013. Ver en http://goo.gl/BjAa20 (Consultado el 13-10-2014)

44 "NSA Whistleblower: 'I Do Not Expect To See Home Again'" Marc Pitzke en Der Spiegel, 10 de junio de 2013. Ver en: http://goo.gl/2e5Xu9 (Consultado el 13-10-2014)

45 "Clapper: Leaks are 'literally gut-wrenching,' leaker being sought", Aaron Blake en The Washington Post. 9 de Junio de 2013. Ver en http://goo.gl/AuT812 (Consultado el 13-10-2014)

46 "Snowden leaks 'worst ever loss to British intelligence", BBC, 11 de octubre de 2013. Ver en: http://goo.gl/zFTKhL (Consultado el 13-10-2014)

47 "Pentagon Says Snowden Took Most U.S. Secrets Ever: Rogers" Chris Strohm y Del Quentin Wilber en Bloomberg News, 9 de enero de 2014. Ver en http://goo.gl/qrbTRo (Consultado el 13-10-2014)

48 "David Miranda row: Seized files 'endanger agents'", BBC News, 30 de agosto de 2013. Ver en: http://goo.gl/wj7xoz (Consultado el 13-10-2014)

49 "Edward Snowden Could Have As Many As 20,000 Australian Intelligence Files", Ben Collins en Business Insider Australia, 5 de dicembre de 2013. Ver en: http://goo.gl/Vp2AeD (Consultado el 13-10-2014)

50 "Edward Snowden: the whistleblower behind the NSA surveillance revelations", Glenn Greenwald, Ewen MacAskill y Laura Poitras, en The Guardian, 9 de junio de 2013. Ver en: http://goo.gl/ZjQxOp (Consultado el 13-10-2014

51 "Estados Unidos espió los teléfonos móviles de 35 líderes mundiales",

Claudi Pérez y Lucía Abellán, El País, 25 de octubre de 2013. Ver en: http://goo.gl/wgJHcW (Consultado el 13-10-2014)

52 "Espionnage de la NSA : tous les documents publiés par "Le Monde"", Le Monde, 21 de octubre de 2013. Ver en: http://goo.gl/uYvnJM (Consultado el 13-10-2014)

53 "The UK Tempora Program Captures Vast Amounts of Data — and Shares with NSA", Philip Bump, The Wire, 21 de junio de 2013. Ver en: http://goo.gl/FtKkVi (Consultado el 13-10-2014)

54 "Révélations sur les écoutes sous-marines de la NSA", Jacques Follorou y Martin Untersinger, Le Monde, 9 de mayo de 2014. Ver en: http://goo.gl/emjrOO (Consultado el 13-10-2014)

55 "Slides about NSA's Upstream collection", Top Level Telecommunications, May 20, 2014.Ver en http://goo.gl/UlvPQG (Consultado el 13-10-2014)

56 "XKeyscore: NSA tool collects 'nearly everything a user does on the internet'", Glenn Greenwald en The Guardian, 31 de Julio de 2013. Ver en: http://goo.gl/SA1j4S (Consultado el 13-10-2014)

57 "NSA collects millions of text messages daily in 'untargeted' global sweep", James Ball, The Guardian, 16 de enero de 2014. Ver en: http://goo.gl/e4op55 (Consultado el 13-10-2014)

58 "Report: NSA 'collected 200m texts per day'", BBC News, 17 de enero de 2014. Ver en: http://goo.gl/PYZDrh (Consultado el 13-10-2014)

59 "How the NSA's MUSCULAR program collects too much data from Yahoo and Google", Barton Gellman y Matt DeLong, The Washington Post, 30 de octubre de 2013. Ver en: http://goo.gl/GC6lLJ (Consultado el 13-10-2014)

60 "How we know the NSA had access to internal Google and Yahoo cloud data", Barton Gellman, Ashkan Soltani, y Andrea Peterson, The Washington Post, 4 de noviembre de 2013. Ver en: http://goo.gl/urkyZV (Consultado el 13-10-2014)

61 "Boundless Informant: the NSA's secret tool to track global surveillance data", Glenn Greenwald y Ewen MacAskill, The Guardian, 11 de Junio de 2013. Ver en: http://goo.gl/XsZTHG (Consultado el 13-10-2014)

62 "Follow the Money': NSA Spies on International Payments", Der Spiegel, 15 de septiembre de 2013. Ver en: http://goo.gl/pZwpUQ (Consultado el 13-10-2014)

63 "Revealed: how US and UK spy agencies defeat internet privacy and security", James Ball, Julian Borger y Glenn Greenwald, The Guardian, 6 de septiembre de 2013. Ver en: http://goo.gl/zyKJbo (Consultado el 13-10-2014)

64 Ente los numerosos artículos técnicos que tratan el tema, resulta de interés el reporte de Sebastián Pop, que se refiere al empleo de microprocesadores espías de Intel en telefonía celular. Ver "Secret 3G Radio in Every Intel vPro CPU Could Steal Your Ideas at Any Time" en http://goo.gl/Y5jdEf (Consultado el 13-10-2014)

65 "Microsoft handed the NSA access to encrypted messages" Glenn Greenwald, Ewen MacAskill, Laura Poitras, Spencer Ackerman y Dominic Rushe, The Guardian, 12 de julio de 2013. Ver en http://goo.gl/UULsO6 (Consultado el 13-10-2014)

66 "A Silent Attack, but Not a Subtle One" John Markoff, en New York Times 26 de septiembre 2010, ver en http://goo.gl/HQNShr (Consultado el 13-10-2014)

67 "Un virus sophistiqué ravive la crainte du cyberterrorisme", Benjamin Ferran, en Le Figaro, 24 de septiembre de 2010. Ver en http://goo.gl/pgHa5U (Consultado el 13-10-2014)

68 Infografía de funcionamiento del gusano informático STUXNET, en IEEE (Institute of Electrical and Electronics Engineers) en http://goo.gl/xcXEcB (Consultado el 13-10-2014)

69 "Meet Gauss: The latest cyber-espionage tool", Larry Dignan, en ZDnet de 9 de agosto de 2012. Ver en: http://goo.gl/hoYW9p (Consultado el 13-10-2014)

70 "Inside TAO: Documents Reveal Top NSA Hacking Unit", Der Spiegel, 29 de diciembre de 2013. Ver en: http://goo.gl/14q4X8 (Consultado el 13-10-2014)

71 "NSA 'hacking unit' infiltrates computers around the world", Ver en: http://goo.gl/Ju8R5T (Consultado el 13-10-2014)