MONOGRAFÍA DEL CRIMEN GLOBAL E INTERNET MONOGRAPH ON GLOBAL CRIME AND THE INTERNET

La arquitectura invisible de Echelon

The invisible architecture of Echelon

DEMANDADO 9-12-2023 **REVISADO** 15-2-2024 **ACEPTADO** 28-2-2024

Patrick Radden Keefe

Periodista de Estados Unidos

Palabras claves: Arquitectura invisible Echelon, vigilancia global

Key Words: Invisible Echelon architecture, global surveillance

RESUMEN La ilegalidad se impone sobre la vida cotidiana, como muestra las risas que mantiene los servicios secretos de la justicia ordinaria

ABSTRACT The Illegality is imposed on daily life, as shown by the laughter maintained by the secret services of ordinary justice

Vigilancia secreta e ilegal de los Estados Unidos y países anglosajones en el mundo actual

Introducción a los despachos secretos norteamericanos del espionaje global

La ilegalidad se impone sobre la vida cotidiana, como muestra las risas que mantiene los servicios secretos de la justicia ordinaria en Estados Unidos.

PRENSA: ¿Está usted confirmando la existencia del sistema Echelon?

> PORTAVOZ DEL DEPARTAMENTO DE ESTADO RICHARD BOUCHER: No.
> PRENSA: ¿Así que no lo confirma?
> BOUCHER: No creo que lo esté haciendo. Tendría que comprobar si lo estoy haciendo, pero no creo que lo esté haciendo (Risa).

(De la transcripción oficial de una información de prensa del Departamento de Estado de Estados Unidos, 11 de mayo de 2001).

Tras el atentado contra las torres gemelas, en febrero de 2003, la policía de Nueva York emprendió una campaña frenética para proteger el metro de la ciudad de un posible ataque terrorista (Rashbaum, 2003, Celona, Hunter, 2003). Se desplegaron por la ciudad dieciséis mil agentes de la ley especialmente adiestrados para combatir el terrorismo. Las autoridades aumentaron el número de patrullas y de puestos de control en una miríada de arterias subterráneas que bombean pasajeros hacia Manhattan y fuera de ella todos los días. Agentes de paisano tomaron posiciones en vagones y andenes montando guardia, y grupos de policías fuertemente armados y con chalecos antibalas, conocidos como Equipos Hércules, bajaron a las estaciones. La policía se hizo cargo de las entradas de los trece túneles de metro submarinos que entran y salen de Manhattan y recorrieron cientos de kilómetros de andenes con detectores de radiación, máscaras antigás y perros adiestrados para descubrir bombas.

¡Qué provocó este súbito frenesí protector del departamento de policía de Nueva York? ¿Qué fue lo que les puso sobre aviso? Una palabra en una conversación interceptada entre terroristas sospechosos: *underground*, con su doble significado en inglés de clandestino y ferrocarril subterráneo.

¿Cuándo se coló en el léxico estadounidense el término *chatter*? Es una palabrita curiosa, inocua y trivial al mismo tiempo en sus connotaciones. Significa murmuraciones o rumores, charla, cháchara, parloteo, el parloteo de un niño. Pero luego, de la noche a la mañana, la palabra adquirió un significado nuevo y amenazador. Y ahora el *chatter*, o escuchas ilegales, de un día determinado es un barómetro del pánico nacional. El *chatter*, lo mismo que las indicaciones meteorológicas en que se basa una previsión del tiempo, advierte si se espera el desastre, si estamos en "alerta" o en "alerta alta", el tono aural preciso del índice de amenaza del día.

Tras un par de meses de *blitzkrieg*, los londinenses aprendieron a vivir con los bombardeos, a distinguir instintivamente entre los alaridos reveladores de la artillería y a bloquear todo lo que no fuese lo que amenazaba con hacerles pedazos. Después del 11 de septiembre de 2001, los estadounidenses han demostrado una capacidad similar de adaptación a un entorno inseguro. El nivel de amenaza diario aún aparece en las noticias, disputando pantalla a los

últimos informes de la bolsa, el tiempo y la fecha. Pero la mayoría de nosotros no pensamos mucho en ello (nos interesa más echar una ojeada a la temperatura para saber si tenemos que ponernos la chaqueta) y lo tratamos como las tonalidades cambiantes de un cardenal que va desapareciendo lentamente. Pero no desaparece; el índice de amenaza sigue ahí, cambia un matiz aquí, un grado allá y parece que sólo oscila siempre entre "elevado" y "grave".

¿Por qué peculiar alquimia determina nuestro gobierno el nivel de terror que tendríamos que sentir un día determinado? ¿Qué fuentes de información alimentan ese boletín del estado de sitio en que nos encontramos? La mayoría de los estadounidenses no tiene la menor idea, y tiende a confiar en el personal y la tecnología que aporta el gobierno. Oímos decir que el *chatter* indicó que el Irak de Sadam Husein estaba produciendo armas de destrucción masiva [que se demostró que era mentira] y que el *chatter* previó[¿] los ataques terroristas del 11 de septiembre de 2001. En las semanas previas a un desastre, se nos dice, surge una pauta (Risen, 2003, 2004). Antes del I I de septiembre, antes del atentado de Bali de octubre de 2002, antes de los atentados suicidas de Riad de noviembre de 2003, hubo un súbito pico en el *chatter*, un crescendo de voces extranjeras. Luego, silencio. Luego, el desastre. Sabemos muy poco de los terroristas de Al Qaeda: su fundamentalismo perverso, su matrimonio mortífero de una filosofía que parece mirar al pasado y unas tecnologías que observan al futuro, su estructura organizativa elusiva y viriforme. Pero hemos llegado a conocer este ritmo metabólico revelador: escuchas; silencio; ataque. El *chatter* se ha convertido en un factor crítico aunque espectral de la vida estadounidense en los primeros años del siglo XXI. Sin embargo son muy pocos los que entienden lo que significa esa palabra. ¿Quién charla? ¿Quién escucha? ¿Cómo hacen para escuchar? Y, quizá lo más importante, ¿hasta qué punto es fidedigna esa escucha como augurio de que se aproxima el desastre [el problema es quien provoca ese desastre: ¿el que habla o el que escucha?]

Brindo ahora una teoría de la conspiración. Estados Unidos es el miembro dominante de una red secreta, de la que forman parte otras cuatro potencias anglófonas (el Reino Unido, Canadá, Australia y Nueva Zelanda), que lleva a cabo escuchas de gente de todo el planeta. El pacto entre esos países se inició hace medio siglo, con un documento secreto cuya existencia no ha sido nunca reconocida

por ninguno de los gobiernos implicados: el acuerdo UKUSA. La red que han creado estos países recoge decenas de miles de millones de llamadas telefónicas, correos electrónicos, faxes y télex todos los días y los distribuye, a través de una serie de canales automatizados, a las partes interesadas de los cinco países. Estados Unidos espía de este modo a sus aliados de la OTAN, y el Reino Unido espía a sus aliados de la Unión Europea: la red está por encima de cualquier otro vínculo de lealtad o afiliación. Cada país tiene leyes que prohíben espiar a sus propios ciudadanos pero que no prohíben que sus aliados espíen a esos mismos ciudadanos… así que, por ejemplo, aquí, en Estados Unidos se puede pedir de cuando en cuando al Reino Unido que vigile a ciudadanos de este país, con el sobreentendido de que si encuentra alguna noticia interesante, se la pase sin ninguna clase de problema.

La tecnología utilizada por estas cinco potencias para interceptar comunicaciones es impresionantemente sofisticada. El reducido vocabulario de la lengua inglesa para describir el acto de escuchar está plagado de anacronismos (Blackstone, 1979: 169). William Blackstone definió en sus *Comentarios a las leyes de Inglaterra* (1765-1769) *eavesdroppers* como aquellos que "se apostan en las paredes de una casa o bajo la ventana o los aleros, para escuchar lo que se dice y sacar luego de ello historias malévolas y calumniosas". La palabra evoca aún el personaje oculto tras una mampara o un biombo de las obras de Shakespeare o de Moliere. Hasta *wiretap*, que vincula la escucha a la manipulación de un cable, es una especie de extraña anomalía: gran parte de la interceptación de comunicaciones del siglo pasado no entrañaba manipular cables sino simplemente cazar señales en el aire.

La inteligencia de señales, o *Sigint (signals intelligence)* en la taquigrafía de los políticos y los espías, es el nombre poco conocido de las escuchas que utilizan hoy los propios espías. Espiar se ha convertido en un juego extraordinariamente refinado, con estaciones de escucha inhalando conversaciones recogidas a través de satélites y de torres de microondas; satélites espías a kilómetros de altura en el espacio que captan frecuencias de radio en tierra; y silenciosos e invisibles gusanos de internet que se aferran como parásitos a los nódulos y cruces de la autopista de la información.

Aunque muchos estadounidenses no saben siquiera que existe, la Agencia de Seguridad Nacional (NSA, según las siglas en inglés), la institución que está al cargo del espionaje electrónico, es mayor

que la CIA y el FBI juntos. De hecho, estos organismos de inteligencia mejor conocidos son insignificantes en comparación. Mientras la CIA tiene aproximadamente veinte mil empleados y un presupuesto de unos tres mil millones de dólares, la NSA cuenta con unos sesenta mil empleados esparcidos por el planeta y se calcula que su presupuesto asciende a los seis mil millones de dólares por año[190]. Las estrechas relaciones que Estados Unidos y el Reino Unido tienen en lo que respecta a la cooperación en Sigint hacen que la NSA tenga una comunicación más fluida con la agencia de escucha británica (Centro de Comunicaciones del Gobierno o GCHQ, según las siglas en inglés) que con la CIA. Se dice que la red anglófona lo escucha absolutamente todo, pero su existencia sigue siendo un secreto... que desconocen en algunos casos hasta los cuerpos legislativos de

[190] Es muy difícil determinar las cifras exactas, pues son secretas y han fluctuado mucho en los últimos veinte años bajaron continuamente después de la guerra y han subido súbitamente después del 11 de septiembre de 2001. El sitio web de la Federación de Científicos Estadounidenses tiene buen material sobre personal y presupuestos de las agencias de inteligencias, aunque es evidente que lo único que puede hacer es conjeturas sobre la información oficial. James Bamford, autoridad civil sobre la NSA, afirma en *Body os secrets* que cada jornada laboral acuden a trabajar a Fort Meade 38.000 empleados, y los informes de la prensa suelen hacer referencia a este número y afirman que la NSA tiene unos 40.000 empleados, Pero Bamford añade que la agencia cuenta con otros 25.000 empleados, destinados en puestos de escucha en el extranjero. Lo cual daría un total de más de 60.000 empleados por la agencia de una u otra forma. Véase James Bamford (2001: 482). Los cálculos más comedidos del presupuesto de la NSA lo sitúan entre los tres mil y los cuatro mil millones de dólares antes del 11 de septiembre, aunque lo más seguro es que haya aumentado de forma significativa en los últimos años. Bob Woodward calcula en *Plan of attack* que el presupuesto de la agencia podría sr de unos seis mil millones de dólares (Bob Woodward, 2004, 213). También merece la pena recordar que las cifras del presupuesto sólo para la NSA son engañosas, porque la Oficina Nacional de Reconocimiento (NRO), la agencia secreta encargada de la construcción y mantenimiento de los satélites estadounidenses, cuenta también con presupuesto anual de unos siete mil millones de dólares (Douglas Pasternak, 2003). Sobre el tema de presupuestos, un buen sitio para empezar es la Federación de Científicos Estadounidenses. Véase "Intelligence agency budgets" (en adelante, el sitio FAS). En cuanto a las cifras de la CIA, el sitio FAS da 20.000, pero de esa cantidad menos de 5.000 se dedican al Directorio de Operaciones, que supervisa el espionaje humano activo (2002). Y menos de 1.100 de ese número corresponden a los agentes destinados al extranjero, Douglas Jehl, "Abundance of caution and years of budgest cuts are seen to limit CIA" (2004).

los países que la dirigen. El nombre en clave de la red es Echelon.

Como cualquier buena teoría de la conspiración, ésta contiene importantes elementos de verdad. Como cualquier buena conspiración, es también infalsable: aunque podría ser imposible demostrar que es todo verdad, es también imposible demostrar que no lo es, y el hecho de que las autoridades emitan desmentidos y se nieguen a comentar el asunto hace que la teoría prospere. Es la fábula parabólica quintaesencial de la era de internet. Se difunde de la forma epidémica que lo hacen las historias en la red y afecta a las angustias compartidas por los que canalizan grandes cantidades de información personal a través de una red, sin un conocimiento sólido de lo segura que es la información en tránsito. Al mismo tiempo, a pesar del carácter supuestamente ilimitado de internet, esta teoría de la conspiración parece haber arraigado en Europa pero no en Estados Unidos. Estas historias sobre Echelon, en la medida en que se han filtrado en la conciencia estadounidense, lo han hecho no a través de la prensa o de los noticiarios de la noche, sino más bien a través del folclore alarmista de la televisión y las novelas. En el popular programa de la *ABC Alias,* el zanquilargo espía Sydney Bristow pugna por introducirse en el sistema Echelon y proclama: "Algunas personas piensan que hay una conspiración, que el gobierno espía a todo el mundo. No hay ninguna conspiración", Cayce Pollard, la heroína de *Pattern Recognition,* el libro de 2003 de William Gibson, se las arregla también para colarse en Echelon, un sistema, escribe Gibson, "que permite escudriñar todo el tráfico de la red".

Cuando me enfrenté por primera vez con historias sobre Echelon, se explicaban no como una fantasía sino como un hecho. Yo era un estudiante graduado en el Reino Unido a finales de los años noventa cuando empezaron a aparecer en la prensa historias sobre Echelon. El cuadro que se pintaba era intrigante: una arquitectura de escuchas espectacular que se extendía reticularmente por todo el globo; una infraestructura invisible mediante la cual un selecto puñado de servicios secretos podía escuchar la charla de las naciones y alcanzar una omnisciencia olímpica, oyéndolo literalmente todo, todo el tiempo. Pese a la geometría aséptica de este sistema, sus contornos eran de una sorprendente imprecisión. No estaba claro si la palabra Echelson se refería a un programa determinado de intercepción por satélite o a todo el sistema de cooperación anglófona de Sigint. Se mencionaba el sistema en unos tonos casi mitológicos, pero la mayoría de los informes confesaban abiertamente que no

estaban elaborados apoyándose en datos contrastados.

Marlow, el narrador de *El corazón de las tinieblas* de Joseph Conrad, estaba obsesionado como un niño con "los espacios en blanco de la Tierra", las regiones del mundo que permanecían sin explorar ni cartografiar en el siglo XIX (Conrad, 1967: 9). En el siglo XX no nos están permitidos ya esos misterios cartográficos tan seductores, pero yo descubrí, cuando empecé a sondear el mundo de la inteligencia de señales, que ocupa una tierra en sombra también sin cartografiar en nuestra conciencia contemporánea.

"Las tecnologías más profundas son las que desaparecen", escribió en I99I el informático Mark Weiser en un artículo fundamental, en el que introdujo la idea de "computación ubicua". "Se entretejen en el entramado de la vida cotidiana hasta que son indiferenciables de ella (Weiser, 1991). En la década y media transcurrida, las tecnologías de las comunicaciones han desaparecido exactamente de ese modo. Damos por supuestos nuestros cables aéreos y nuestros teléfonos móviles celulares, los buscas bidireccionales y los ordenadores portátiles inalámbricos. Cuando Weiser escribía eso, el teléfono era algo conectado a la pared por lo que se peleaban los adolescentes, e internet era para unos cuantos una idea, un rumor, y para la inmensa mayoría algo más próximo a la ciencia ficción. Hoy, nuestra relación con la tecnología es umbilical: mi generación fue la primera que llegó a la universidad y se encontró conexiones de internet dispuestas en todos los dormitorios; no podemos vivir, ni siquiera imaginar la vida, sin acceso a la red. No es sólo que utilicemos a diario esa tecnología, sino que transmitimos también más información de la que se haya transmitido nunca a través de los cables y por las ondas: pagamos nuestras facturas y nuestros impuestos por internet; nos reunimos, nos citamos y conversamos electrónicamente; investigamos la trascendencia de los síntomas médicos en la red; y formulamos las preguntas y los dilemas más embarazosos y reveladores en Google, todo en línea. Tenemos una impresión intuitiva de que este medio, que hemos interiorizado hasta el punto de que es casi una prolongación orgánica de nuestros pensamientos y palabras, es vulnerable a la interceptación: alguien podría estar escuchando. Pero para la mayoría de nosotros esta sensación incómoda no pasa de ser una corazonada sin fundamento, uno de los azares extraños de la vida en la era digital.

El presente texto es la historia de los esfuerzos que hice para de-

terminar cómo funciona el *chatter*: quiénes pueden escuchar y cómo lo hacen. Es la historia de una lucha épica entre dos conceptos abstractos (seguridad e intimidad) que se está librando en medio de un cambio social y tecnológico de rapidez relampagueante. Es también una historia del secretismo gubernamental. Mis esfuerzos para cartografiar el mundo secreto de la inteligencia de señales se vieron frustrados por algo que he acabado considerando el postulado de Sigint: hay una proporción inversa entre lo que está dispuesta a decir una persona de la inteligencia de señales y lo que sabe realmente esa persona. Los márgenes del mundo de Sigint están poblados por teóricos de la conspiración y defensores de la intimidad, paranoicos y chiflados, por personajes pintorescos de dudosa credibilidad. Y el centro de ese mundo, el sanctasanctórum ultra secreto del estamento que controla los servicios secretos estadounidenses, alberga la tribu profesional más reservada y sigilosa del mundo: los propios escuchas.

Estados Unidos tiene hoy menos de cinco mil espías actuando en el mundo, pero tiene unos treinta mil individuos dedicados a escuchar. Los satélites de la NSA recogen cada tres horas información suficiente para llenar la Biblioteca del Congreso. Y sin embargo la mayoría de los habitantes del país no tienen casi ninguna información sobre nuestro aparato de escucha global. En consecuencia, carecemos de vocabulario para analizar si nuestros servicios de inteligencia velan adecuadamente por nuestra seguridad o si invaden nuestra intimidad, o ambas cuestiones a la vez. Tendemos a tragarnos enteros conceptos como *intimidad y seguridad nacional*, a considerarlos absolutos indiferenciados e indeterminados, y a negarnos (porque tenemos demasiada poca información o simplemente porque es demasiado difícil) a considerar los diversos cambios que se producen en nuestra sociedad en relación con la matriz libertad-seguridad. No tenemos ni idea de lo fidedigno que es en realidad un índice de seguridad en el *chatter* o si nuestras operaciones de escucha valen los miles de millones de dólares que dedicamos a ellas. No sabemos si existe Echelon y, en el caso de que exista, cómo opera esa red enigmática. Sigue siendo todo un misterio.

No soy un periodista de investigación, ni por inclinación ni por formación. Cuando me puse a ver lo que podía descubrir sobre el espionaje global, lo hice como cualquier civil curioso. Lo que descubrí cuando empecé a husmear en los procedimientos a través de los

cuales Estados Unidos y sus aliados interceptan comunicaciones es que el sistema es como una especie de ventana que da a una serie de asuntos y dilemas más amplios, de los que constituye una metáfora, que serán las luchas definitorias de nuestra era: la negociación entre intimidad y seguridad nacional en un mundo conectado; la profusión de teorías de la conspiración y de paranoia en la era de internet, en que el rumor abunda pero es escaso el suministro de información sólida; y los peligros reales del secretismo oficial sin frenos. Tenía poca idea cuando empecé de que esta búsqueda de información me llevaría a una inmensa "base de escucha" de los brezales ingleses de Yorkshire, y de allí al seno de la Europa burocrática de Bruselas, desde las habitaciones traseras de Washington a los cafés de Copenhague, a una base abandonada de la NSA, oculta en las montañas Smoky de Carolina del Norte. Ni tenía idea de que me enfrentaría a una clase de personajes tan extraña y memorable: espías que se pasan la vida escuchando por auriculares las conversaciones privadas de individuos de todo el planeta; manifestantes, piratas informáticos y militantes que están convencidos de que la intimidad que conocimos en otros tiempos ha dejado ya de existir; funcionarios que sostienen que hasta el simple hecho de hablar de la capacidad de escucha de Estados Unidos equivale a ayudar a los terroristas; y un pequeño grupo de periodistas e investigadores intrépidos que han luchado, a lo largo de las tres últimas décadas, por sacar a la luz, detalle a detalle, el mundo del espionaje global.

Radomos en el desiertp, radomos en el brezal

La arquitectura invisible de Echelon

No puedes evitar darte cuenta de la yuxtaposición. Aquí, lejos del mundo, en medio de prados ondulantes, en una extensión de tierra en que el aire huele a boñiga de vaca, es donde está la estación de escucha más avanzada del planeta. Los brezales ingleses del norte de Yorkshire son después de todo país de vacas. Tras abandonar la elegante población balnearia victoriana de Harrogate, mi taxi gira hacia al oeste y atraviesa unos doce kilómetros de verdes campos. El tráfico disminuye al salir de la ciudad y los coches con los que nos encontramos parecen ir mucho más despacio de lo que necesitan ir, a un ritmo agrario y deliberado. Los campos están separados por una red de setos bajo un cielo panorámico sin nubes. Se congregan

aquí y allá ovejas, y docenas de vacas que haraganean junto a paredones de piedra que se desmigajan; algunas nos miran pasar, otras rumian, ajenas a todo.

Me han prevenido, he visto fotos... sé lo que espero encontrar. Pero cuando surge a la vista la primera cúpula, se me corta la respiración. La bucólica carretera serpentea y sube y baja y cuando volvemos a ascender y descender y coronamos una colina se hace visible a los lejos la punta de una gran esfera blanca, que resplandece en el calor estival. Una cúpula gigante salpicada de hoyuelos, una gran pelota de golf Kevlar. Luego, de pronto, cuatro cúpulas y luego ocho, mientras otras afloran a la vista sobre la colina. La carretera desciende y vuelven a desaparecer y después afloran visibles de nuevo.

Mientras el taxi rodea la valla del perímetro, la base se hace presente en relampagueos a través de una hilera de árboles. Los globos blancos se llaman radomos, y cada uno de ellos alberga una antena parabólica, protegiéndola de los elementos y ocultando su orientación: la cúpula en sí no es más que una especie de piel. Cuento veintiocho de esas cúpulas en total, de un blanco fantasmal que contrasta con el verde del campo. Parecen ultraterrenas.

Y en cierto modo, lo son. Las parabólicas están escondidas dentro de los radomos porque sus focos supersensibles están dirigidos hacia una serie correspondiente de satélites que se ciernen a más de treinta mil kilómetros de altura. Algunos son satélites de comunicaciones que transmiten mensajes seguros a otras instalaciones de los servicios de inteligencia repartidas por el mundo. Otros son satélites espías, que sacan fotografías, interceptan comunicaciones y utilizan Sistemas de Posicionamiento Global para señalar los emplazamientos de personas o vehículos diversos por todo el planeta. Y algunos son satélites de comunicaciones comerciales corrientes, como los transmiten las llamadas telefónicas y el tráfico de internet a través los océanos. Las dos primeras variedades de satélites se construyeron específicamente para que se correspondieran con la base. Este tercer tipo, sin embargo, no. Estos satélites los maneja una empresa llamada Intelsat, y las señales que transmiten son comunicaciones civiles privadas. Pero la base recoge también esas señales, interceptando silenciosa e incesantemente grandes flujos de comunicaciones privadas por minuto hora tras hora. El letrero de la entrada dice: RAFf Menwith Hill.

Me acerco a la entrada protegida con sacos de arena, sonrío a los

serios policías militares británicos que hacen guardia y atisbo dentro. RAF significa Royal Air Force, es decir, Real Fuerza Aérea, las fuerzas aéreas británicas, pero el nombre es un equívoco deliberado. La base se construyó en los años cincuenta en terreno comprado por la corona británica, pero en 1966 la propiedad fue adquirida por NSA, Agencia de Seguridad Nacional estadounidense. Así que bien la estación es nominalmente una base de la RAF, alberga en realidad a más de mil doscientos estadounidenses. Esta gente vive en casas que hay dentro del perímetro de la valla, envía a sus hijos a la cuela de primaria y secundaria dentro de la valla, envía a sus hijos a la escuela de primaria y secundaria dentro de la valla, utiliza una tienda propia, una oficina de correos, un centro deportivo, un bar y una bolera, todo dentro de la valla. La bolera, en una nomenclatura discutible tratándose de una base relacionada con el programa nuclear de Estados Unidos, se llama Zona de Impacto. Hay casas y una capilla y una zona de juegos y una pista y un campo de béisbol de dimensiones reglamentarias. La base ocupa unos quinientos sesenta acres. Soldados armados y con perros patrullan la valla por detrás de una cinta serpenteante de alambre espinoso.

Aunque, en esta era de proyección del poder estadounidense, estamos acostumbrados a la idea de personal militar permanente viviendo en un enclave de este tipo en el extranjero, me quedé sorprendido al enterarme de que la mayoría de los empleados de la base son en realidad civiles: ingenieros, técnicos, matemáticos, lingüistas y analistas. La NSA ha contratado siempre gran número de civiles: profesionales, generalmente con formación técnica, que superan las rigurosas exigencias curriculares y de seguridad con las que han de cumplir los quieran trabajar en la primera línea del campo más secreto de los servicios de inteligencia estadounidenses. Estas personas proceden empresas tecnológicas y aeroespaciales que obtienen contratas regulares del gobierno. Trasladan a la base sus pertenencias y sus familias, atraídos por los sobresueldos y los complementos: vivienda gratis, transporte gratuito de mobiliario y coches y, sobre todo, un sueldo libre de impuestos[191]. Trabajan en

[191] Un artículo de Bárbara E. Scott publicado en el número de abril de 1991 del boletín interno *NSA Newslatter* anuncia una semana de reclutamiento en Fort Meade y sugiere que la pregunta para "quienes buscan variedad de experiencias, la oportunidad de vivir en una cultura diferente, maravillosas oportunidades de viajar a países exóticos e incluso de ahorrar dinero, sería: "¿Por qué no hacer una gira campestre?".

tres turnos de ocho horas, para que la gran máquina de interceptación no deje de funcionar. Trabajan el el día de navidad, el día de año nuevo y durante las manifestaciones habituales que tienen lugar a la entrada de la base el 4 de julio. Hay traductores que saben árabe, persa, hebreo y todos los idiomas europeos[192]. Con unos cuatrocientos empleados más del Ministerio de Defensa británico, esta estación de espionaje silenciosa y activa, de la que la inmensa mayoría de los civiles estadounidenses y británicos nunca han oído hablar, tiene una nómina tan grande como todo el servicio de inteligencia nacional inglés, el MI_5.

En el mesón Black Bull, un bar local, la noche antes de la visita a la base, un par de adolescentes que estaban tomando pintas de cerveza y comiendo patatas fritas con sabor a pollo al curry en la barra bromeaban sobre los coches cargados de bellas y jóvenes americanas, "las chicas de Menwith Hill", a las que ven de vez en cuando. Las mujeres conducen coches americanos con el volante a la izquierda y se desplazan los fines de semana a los bares de los pueblos del entorno, o Harrogate o a York y luego regresan para desaparecer detrás de valla. Si la vida social de esas mujeres tiene el carácter de una aparición para los locales, su vida profesional es más misteriosa aún. Uno de los chicos de la barra, delgado como un junco y de cabello oscuro, con un aro en la ceja, dijo que él había trabajado en "la colina" un tiempo, en la cafetería, pero que la base estaba segregada en la "colina alta" y la "colina baja", que había una división estricta entre las zonas residenciales y las zonas de trabajo, y que su autorización de seguridad, que había exigido por sí sola un montón de formularios, preguntas, comprobaciones y pruebas, no le permitía aproximarse a la actividad real que se desarrollaba en la base. Dijo que por lo que él había podido ver, gran parte del trabajo se realiza en las incalculables extensiones de la base que están bajo tierra. "Pero por lo que yo he oído –dijo, enarcando una ceja conspiratoria y mirando mi cuaderno para cerciorarse de que tomaba nota-, es una zona de control de extraterrestres" (Graham, Nussbaum, 2004: 86) [193]. Sus compañeros se echaron a reír al oír

[192] Duncan Campbell, *Interception capabilities 2000,* informe al director general de investigación del Parlamento Europeo, 1999.

[193] El senador demócrata por Florida, Bob Graham, que visitó la base con otros miembros de los comités de inteligencia del Congreso en el verano de 2001, nos ofrece la siguiente descripción, rara aunque no demasiado reveladora, del interior de Menwith Hill:

El interior del complejo era una serie de amplios espacios abiertos, ocupa-

esto y aún más cuando vieron que yo lo anotaba diligentemente.

Estoy parado junto a la entrada, estirando el cuello y mirando a través de la valla. Los guardias empuñan ametralladoras y me miran con una curiosidad perezosa. Una pantalla digital que hay al lado una agrupación de edificios bajos parpadea mensajes a los coches que entran en la base. "Reiki y masaje martes noche; seguro Geico todos los jueves; karaoke jueves noche; beber y conducir destroza vidas".

Uno de los guardias carraspea:
-Perdón, señor.
Cabecea para indicar algo a mi espalda.

Hay un sedán azul parado, esperando para pasar. Me hago a lado. Lo conduce una joven que viste una camiseta con el pelo hacia atrás. Nos miramos un segundo. Es aproximadamente mi edad... ¡una chica de Menwith Hill! Los guardias le indican que pase y desaparece.

Dentro de la valla, en edificios sin ventanas de una sola planta y en sótanos subterráneos de alta tecnología, las chicas de Menwith Hill trabajan con sus colegas en la interceptación clandestina de miles de millones de comunicaciones por día. Se ha afirmado que la base intercepta todo el tráfico de las telecomunicaciones que entran y salen de Europa y que pasan por Inglaterra.

Éste es el rostro inescrutable del espionaje estadounidense en el siglo XXI. La caída del Telón de Acero causó una ruptura en la geografía establecida de Europa y del mundo que desencadenó un lento cambio tectónico que todavía sigue modificando el paisaje geopolítico. El final de la guerra fría modificó también la naturaleza de

---

dos por centenares de personas, en grupos de unas veinticinco según la misión. Cada grupo se dividía en dos áreas: los técnicos, que atendían los complejos sistemas informáticos que recogían la información, y los analistas, que seleccionaban por prioridad los datos y los estudiaban. Mientras recorríamos el complejo, vimos a los analistas enfrascados en datos que llegaban de miles de kilómetros de distancia, incluidas observaciones en tiempo real de sucesos que requerían vigilancia del personal de Menwith Hill. Claro que eso no era tan obvio para nosotros. Un empleado pulsaba una tecla y decía: "¡Mira esto!" Y veíamos una serie de líneas serpenteantes que para el personal de Menwith contenían un mundo de información. Esa información podría ser más importante que el armamento de este nuevo siglo (Graham, Nussbaum, 2004, 86).

las actividades del espionaje para Estados Unidos y sus aliados. La descentralización de la amenaza que habían planteado los soviéticos, unida a un un presupuesto de defensa más reducido, una nueva sensación de optimismo y una menor tolerancia estadounidense a las bajas militares, condujo a una acusada disminución del número de espías humanos en activo. Han desaparecido los espías de gabardina de las novelas de John le Carré. situados en la vanguardia del espionaje de la guerra fría, a los que se enviaba a infiltrarse en el campo enemigo o que trabajaban desde las embajadas, reclutaban topos y agentes dobles y arriesgaban la vida en el proceso. El espionaje humano, o Humint, estaba ya en firme decadencia al final de la guerra fría y su carácter prioritario siguió reduciéndose en Estados Unidos durante los años noventa. En 1198 Porter Goss, el congresista de Florida y antiguo agente de la CIA que fue director del Comité de los Servicios de Inteligencia de la Cámara de Representantes y que en septiembre de 2004 fue nombrado director de la CIA, declaró simplemente: "Es justo decir que en el área del espionaje humano el aparador está casi vacío" (Pincus, 1998).

Pero aunque los políticos estadounidenses no estuviesen dispuestos a sacrificar vidas de espías en países que no desempeñaban ya un papel decisivo contra los soviéticos o las de militares en lugares como Mogadiscio o Sarajevo, estaban más que dispuestos a invertir en nuevas tecnologías para las guerras y para recoger información secreta por control remoto, como si dijésemos. Las administraciones de George H. W. Bush y Bill Clinton dejaron claro en una serie de conflictos que Estados Unidos, siempre que fuese posible, prefería usar artefactos en vez de seres humanos. En palabras del antiguo agente de la CIA Robert Baer, "La teoría era que los satélites, internet, la interceptación electrónica, incluso las publicaciones académicas nos explicarían todo lo que necesitábamos saber sobre lo que pasaba al otro lado de nuestras fronteras" (Baer, 2002: XVII).

En realidad, esta tendencia no era nada nuevo. Desde los años setenta había habido una sensación creciente de que cuando la tecnología avanzase, podría desplazar al agente que actuaba sobre el terreno. Stansfield Turner, director de la CIA con Jimmy Carter, se reunía con éste dos veces por semana para informarle sobre los diversos tipos de recolección de informaciones secretas que practicaba Estados Unidos. Turner pensaba que el presidente y él compartían una "tendencia técnica" y comentaba que los dos habían acabado considerando básicamente anticuado al "espía humano

tradicional" (Andrew, 1995: 429).

Pero lo que era una corazonada en el caso de estos dos hombres convirtió en una convicción para las administraciones siguientes, en las que una combinación de artilugios y dinero parecieron aportar un medio de no tener que enviar agentes en misiones arriesgadas. En el número de julio-agosto de 2001 de la *Atlantic Monthly*, sólo unas semanas antes de los ataques terroristas del 11 de septiembre, un antiguo agente de la CIA llamado Reuel Marc Gerecht publicó un artículo en el que deploraba la ausencia total de espionaje humano eficaz sobre el terreno en Oriente Próximo. "A menos -concluía- que uno de los peones de Bin Laden cruce la puerta de una embajada o un consulado de Estados Unidos, son extremadamente remotas las posibilidades de que un agente antiterrorista de la CIA vea uno alguna vez" (Gerecht, 2001).

Desde la fundación de la NSA, hace más de medio siglo, ha imperado la idea de que mientras que el mundo de las actividades de inteligencia era muy secreto y no era algo que debiese discutirse con quien no estuviese en el tema, el mundo de la inteligencia de señales más secreto de todos. Se puede detectar esta jerarquía de secretismo incluso en los chistes habituales sobre las agencias relacionadas. La vieja broma sobre la NSA (que fue creada no por el Congreso sino por el presidente Harry Truman en una orden ejecutiva secreta del 24 de octubre de 1952) era que sus iniciales significaban *"No such agency"*; es decir, "ninguna agencia tal" o *"Never say anything"*, o "nunca digas nada". Este mantra debió de adoptarse con entusiasmo desde el principio, porque durante las dos primeras décadas de su existencia la NSA no fue reconocida por el gobierno federal y no apareció en ninguno de los presupuestos anuales de los servicios federales de inteligencia; figurando sus asignaciones sepultadas en otros apartados que no llamaban la atención. Esto pese al hecho de que por entonces la agencia tenía más de diez mil empleados (Kahn, 1996: 677-689). Por el contrario, el chiste que circulaba sobre la Oficina de Servicios Estratégicos, la predecesora de la CIA, que hace espionaje humano, era que OSS –sus siglas en inglés- significaba "Oh so social", es decir, "Oh, tan social". Esto puede explicar por qué la mayoría de los estadounidenses pueden decirte bastante sobre la CIA hoy, mientras que un número sorprendente de ellos nunca ha oído hablar de la NSA. Pocos podrían decirte lo que hace o dónde está localizada. Raras veces

se habla de ella en la prensa y, a pesar de los muchos comentarios sobre el *chatter* en los noticiarios de la noche, el acrónimo NSA incide muy poco en la conciencia del estadounidense medio.

La NSA opera desde su cuartel general de Fort Meade, Maryland, un enorme edificio de cristal negro reflectante. Hasta la arquitectura del "Puzzle Palace", como se le llama a veces, desbarata los intentos de imaginar lo que está pasando dentro. Es literalmente una caja negra. Sabemos que la agencia tiene empleados más matemáticos que ninguna otra organización del mundo y que el campus de Fort Meade es la concentración más densa de capacidad informática del planeta. Sólo uno de los superordenadores Cray de la agencia secreta puede manejar 64.000 millones de instrucciones individuales por segundo.

El trabajo de la NSA está dividido en dos funciones: seguridad de comunicaciones e inteligencia de señales. El primero entraña crear comunicaciones seguras y criptografías para los dirigentes políticos del país y para los militares[194]. La segunda responsabilidad se basa en la escucha. El hecho de que sea difícil conseguir información sobre la NSA se debe en parte a que la agencia no es usuaria de su propia información secreta. No hay agentes de la NSA armados sobre el terreno que utilicen la información secreta que ha recogido la agencia. El Puzzle Palace sólo proporciona información a otras agencias y a políticos y generales. Es, en ese sentido, pasiva. Simplemente se sienta y escucha[195].

El motivo de todo este secretismo es evidente: la escucha sólo funciona si la persona a la que estás controlando no sabe que está siendo controlada. Cuando la prensa informó en 1998 de que el

[194] En realidad, Sigint es un término que abarca una serie de "ints" o medios de inteligencia subsidiarios. Suele aludirse a la interceptación de comunicaciones más específicamente como Comint o inteligencia de comunicaciones. Otros tipos de Sigint son Imint (imagineria), Radint (radar), Elint (electrónica), etcétera.

[195] Esta característica organizativa concreta caería en realidad bajo el fuego de la Comisión del 11-S en su informe final: "La NSA no creía que fuese labor suya investigar las identidades [de presuntos terroristas]. Se consideraba una agencia de apoyo a las que consumen inteligencia, como la CIA. La NSA procuró responder resueltamente a todas las peticiones. Pero esperó a que le peguntaran". Comisión Nacional sobre ataques terroristas a los Estados Unidos, *The 9/11 report: final report of the national commisssion on terrorist attacks upon the United States* (Norton, 2004: 353) (en adelante *9/11 Commission report*).

espionaje estadounidense estaba interceptando las conversaciones por teléfono de satélite de Osama Bin Laden, éste dejó inmediatamente de utilizar ese teléfono (Pincus, 2002)[196]. La lección está clara: cuando tu presa sabe que puedes descifrar su código, ideará uno nuevo. Aún es peor toda la cadena de posibilidades de engaño deliberado. Después de que picos de *chatter* terrorista desencadenasen una serie de alarmas sobre ataques terroristas inminentes en diversos lugares del mundo en 2003, algunos observadores de la comunidad de los servicios de espionaje pensaron que Al Qaeda tal vez estuviese lanzando señuelos deliberadamente en frecuencias que sabía que estaban controladas por la NSA.

Los nuevos espías no son como James Bond o George Smiley. No son individuos duchos en el manejo de las armas y amigos de la juega, agentes solitarios arrojados en paracaídas en territorio extranjero. Los nuevos espías son las chicas de Menwith Hill: elegantes, motivadas, del lado carca y pijo quizá, más familiarizadas con un teclado ergonómico que con una cámara oculta en un reloj de pulsera. En Menwith Hill se encuentran todas las contradicciones del nuevo espionaje. Una base de la era espacial, que se alza cinematográficamente con la amplitud y el cielo de la campiña de Yorkshire como fondo. Una microcomunidad de estadounidenses, cerrada en sí misma y reservada, en el corazón de Gran Bretaña. Dos docenas de antenas parabólicas, ocultas dentro de sus membranas como capullos de gusanos de seda, enfocadas hacia satélites situados a una altura de miles de kilómetros. Y todo eso en la vieja calzada romana que lleva a York, una calzada construida porque los romanos sabían que construir y controlar las vías de comunicación era clave para mantener un imperio. Mientras que el éxito del espionaje se apoyaba tradicionalmente en la capacidad para entrar "en" o "dentro" (infiltrarse), en el nuevo mundo de los servicios de inteligencia una oscura base en la otra punta del planeta puede tener tanto o más valor para las operaciones militares como un

[196] Véase un relato del momento en que Bin Laden se deshizo del teléfono en Steve Coll (2002); también se puede atender a la terrorífica historia de Coll sobre las operaciones de la CIA en Afganistán y la aparición de Al Qaeda: *GhostWars* (2004). El artículo original que contenía la información filtrada era "Inside the ring", de Ernest Blazar (1998). Michael Scheuer, autor de *Imperial hubris,* arremete contra Blazar y los otros periodistas que publican filtraciones y los funcionarios que las proporcionan, argumentando que esta actividad equivale a traición (2004: 192-200).

agente en una embajada. Por ejemplo, no fue una base desplazada a Arabia Saudí la que recibió el premio Estación del año de la NSA en 1991 por su papel en la guerra del Golfo, sino la RAF Menwith Hill, situada a miles de kilómetros de distancia" (Hager, 1996: 40).

Y Menwith Hill es sólo la más grande de las estaciones de escucha, el punto más brillante de una constelación de bases grandes y pequeñas, con torres de microondas y antenas parabólicas apuntando al cielo: Bad Aibling en Alemania; la base aérea de Misawa en Japón; Akrotiri en Chipre; Guantánamo en Cuba; y Pine Gap, en el centro mismo de Australia. Estas bases, a pesar de estar localizadas en países extranjeros, con el pleno consentimiento de sus diversos gobiernos nacionales, están dirigidas por estadounidenses. La mayoría de los países anfitriones tienen cierta base racional persuasiva para aceptarlas: una estrecha alianza militar con Estados Unidos, con la promesa tácita o explícita de protección militar estadounidense, si alguna vez se necesitase; compartir cierta cantidad de información secreta, por la que la agencia arrendataria comunica al gobierno anfitrión cualquier dato valioso recogido; o a menudo simplemente dinero. Estados Unidos, para mantener una base en un lugar estratégico del mundo en que pueden captarse en el aire abundante señales, está dispuesto a pagar rentas generosas, y la presencia de centenares o miles de militares y civiles estadounidenses nunca ha sido mala para la economía en las regiones remotas en que la NSA tiende a instalarse.

Hasta los aliados más estrechos de Estados Unidos en cuestiones de inteligencia (el Reino Unido, Canadá, Australia y Nueva Zelanda) tienen una cuantía limitada de participación en el funcionamiento de esas bases. Es cierto que hay representantes del gobierno anfitrión presentes al otro lado de la valla, y que a veces su papel es sustancial: ayudan a operar y mantener en funcionamiento el equipo de interceptación o analizar los resultados. Pero el papel de estos agentes ha tenido a ser de mera custodia. En un juicio celebrado en los años setenta, un agente británico que trabajaba en RAF Edzell, una estación de escucha estadounidense situada en una zona agrícola del sur de Aberdeen (Escocia), dijo: "Soy el único agente británico de la bases. No sé lo que se hace. No conozco detalles de las operaciones. No tengo ninguna participación en ellas. Estoy completamente aislado. Mis colegas estadounidenses no me hablan". Otro dijo simplemente: "Soy el único representante del casero" (Robertson, 1998: 125).

Bajo la jefatura de Estados Unidos, cinco agencias de espionaje –el Centro de Comunicaciones del gobierno (GCHQ) de Inglaterra, el Centro de Seguridad de Comunicaciones (CSE) de Canadá, el Directorio de Señales de la Defensa (DSD) de Australia, el Centro Seguridad de Comunicaciones del Gobierno (GCSB) de Nueva Zelanda y la NSA- han envuelto la Tierra con una red espectral de vigilancia electrónica. Los detalles de esta asociación íntima los conocen muy pocos. Los políticos no llegan a entenderla plenamente en nombre de la prevención y de la seguridad, los servicios de inteligencia mantienen en la oscuridad a los comités supervisores del estado. Ni siquiera lo entienden del todo los propios escuchas. Dentro de las agencias de Sigint el conocimiento de las cosas se asigna estrictamente sobre la base de lo que se necesita saber, y los universos profesionales de los empleados de Sigint se reducen a los parámetros de sus tareas compartimentadas concretas. Un criptoanalista puede toda su carrera profesional en la NSA y no enterarse siquiera del nombre cifrado del programa que suena de fondo en el pasillo y que han estado utilizando todo el tiempo colegas suyos. El público sólo conoce este tipo de actividades de inteligencia anecdóticamente: las especulaciones oídas a medias de paranoicos vociferantes, los pronósticos alarmistas y algún artículo de fondo de la prensa, la continua reificación de rumores sobre internet. Y esa palabra única y recurrente, lírica y rotunda al mismo tiempo, que invoca la naturaleza arquitectónica del sistema y también la jerarquía rigurosa de lo que se necesita saber: Echelon.

Cuando Henry Lewis Stimson fue nombrado secretario de estado por el presidente Herbert Hoover en I929 y se enteró de que los descifradores de códigos estadounidenses habían estado interceptando y leyendo las comunicaciones de diplomáticos británicos, franceses, italianos y japoneses, se quedó sobrecogido y pronunció estas palabras que se hicieron famosas: “Un caballero no lee la correspondencia de otro”. Pese a la delicadeza de Stimson, la intercepción de comunicaciones probablemente sea tan antigua como la comunicación.

El mejor modo de cartografiar la historia de la interceptación de comunicaciones es explorar la historia de los intentos de preservar la confidencialidad de los mensajes, es decir, la historia de la cripto-

grafía[197]. La gente sabía ya transformar u ocultar bastante bien los mensajes confidenciales que quería enviar incluso en las formas más antiguas de comunicación escrita. David Kahn, el especialista más destacado del mundo en la historia de la criptografía, afirma en *The codebreakers,* su obra magistral de mil páginas, que la criptografía es, a su manera, tan natural e inevitable en su evolución como el lenguaje mismo. "Debe ser que en cuanto la cultura ha llegado a un cierto nivel, probablemente medido sobre todo por su alfabetismo, aparece de forma espontánea la criptografía… como lo hicieron también, probablemente, sus padres, el lenguaje y la escritura –escribe Kahn-. Las múltiples necesidades y deseos humanos que exigen intimidad entre dos o más personas en medio de la vida social deben conducir inevitablemente a la criptografía, siempre que las personas prosperen y siempre que escriban" (Kahn, 1996: 84). Kahn rechaza la idea de que la escritura secreta se propagase de continente a continente por algún proceso de difusión cultural, como se puede demostrar que hicieron tantas otras innovaciones técnicas, y afirma en lugar de eso que la presencia de toscos métodos de cifrado incluso en países lejanos y aislados sólo puede indicar una aparición espontánea y orgánica.

Heródoto nos cuenta en su *Historia* que el tirano Histieo estaba en la corte persa del rey Darío y quería enviar un mensaje a su yerno, Aristágoras, para instarle a rebelarse contra los persas (Heródoto, 1987, 5: 35). Era muy arriesgado, en embargo, enviar un mensaje tan delicado a Mileto, donde estaba Aristágoras, con todos los caminos vigilados. Así que Histieo llamó a su esclavo de más confianza, le afeitó la cabeza y le tatuó el mensaje en el cuero cabelludo. Luego esperó y cuando le volvió a crecer el pelo al esclavo le envió a ver a Aristágoras con la orden de que sólo le dijese una cosa: "Aféitame la cabeza". En la China antigua, los mensajes confidenciales se escribían en finas láminas de seda o de papel y se enrollaban luego en una bola que se cubría de cera (Kahn, 1996: 73). El mensajero ocultaba la bola en la ropa o en el recto, o en el estómago, y sólo se la entregaba al receptor previsto. En realidad, ninguno de estos

[197] Igual que con el término "Sigint", cuando empleo "criptografía" agrupo por conveniencia una serie de términos técnicos diferentes bajo el mismo paraguas semántico. Con criptografía me refiero al arte de hacer y deshacer códigos y claves en el sentido más amplio. Para un análisis más matizado de las diferencias criptografía, criptología, estegamografía y demás, ahóndese en Kahn, *Codebreakers.*

métodos es per se criptografía (Singh, 1999: 15). Mientras la palabra criptografía se deriva del griego "kryptos", que significa "oculto", y de "graphein", que equivale a "escribir", estos subterfugios eran más bien lo que se conoce como esteganografía, o "escritura encubierta", por la palabra griega, que significa "encubierto". La verdadera elaboración y desciframiento de códigos se desarrolló más tarde, en el siglo IX, entre los árabes. Los creadores del criptoanálisis (la ciencia de desentrañar un mensaje cifrado sin la clave del código) fueron los sabios árabes de la Edad Media.

Pero lo que estimuló realmente el progreso de la criptografía fue aumento de las relaciones diplomáticas que se produjo en la Edad Media y el Renacimiento y la paralela interceptación de comunicación diplomáticas. A principios del siglo XVI, los estados europeos empezaron a nombrar embajadores que debían vivir en otras cortes (Kahn, 1996: 109). Los embajadores enviaban informes a sus países, y estos documentos eran a veces abiertos y leídos. A finales del siglo XVI, ese juego del gato y el ratón de la interceptación diplomática había llegado a adquirir tanta importancia que la mayoría de los estados tenían "secretarios de cifras" permanentes dedicados a cifrar los mensajes que se enviaban, a descifrar los que llegaban y a intentar desentrañar los códigos de los mensajes interceptados. Estos primeros descifradores profesionales a jornada completa fueron los antecedentes directos de los analistas e ingenieros del Menwith Hill de hoy.

En la Venecia del Renacimiento, el secretario de cifras de la era un hombre de prestigio y de gran importancia política. Se llamaba Giovanni Soro, y tenía tanta fama como descifrador de códigos que ya en 1510 la curia papal le enviaba los mensajes cifrados que nadie era capaz de descifrar en Roma (Kahn, 1996: 109). Venecia estaba bajo el control del Consejo de los Diez, el misterioso cuadro de funcionarios que mantenía el orden con una policía secreta autoritaria y numerosos informadores, y descifrar códigos adquirió una importancia nueva. Soro trabajaba con dos ayudantes en una habitación situada encima de la Sala di Segret del palacio del Dux. Las puertas que daban a sus cámaras estaban enrejadas. Cuando se interceptaban mensajes cifrados dirigidos a potencias extranjeras, se enviaban directamente a Soro y a sus ayudantes. Se dice que a los secretarios de cifras no se les permitía abandonar el lugar de trabajo hasta que habían descifrado el código. La operación tuvo tanto éxito que pu-

sieron en marcha una pequeña escuela de desciframiento de códigos en la que había exámenes todos los años en septiembre. Ésta fue, tal vez, la primera Cámara Negra, que es el nombre que se les ha dado a las pequeñas unidades secretas de interceptación y criptografía de gobiernos posteriores. Desde la habitación del palacio del Dux hasta la literal cámara negre, el gran Puzzle Palace negro de Fort Mead, estas operaciones han compartido notorias similitudes.

En el siglo XVII, el desciframiento de códigos estaba reconocido generalizadamente como una actividad vital para la preservación del poder oficial. Antoine Rossignol, un descifrador francés de mucho talento que atrajo la atención del cardenal Richelieu, se convirtió en una pequeña celebridad en la corte de Luis XIV (Kahn, 1996: 159). Trabajaba en una habitación situada al lado del estudio del rey Sol en Versalles, en la sede misma de la monarquía. Tan crucial era Rossignol para el predominio de Francia, que se convirtió en un hombre rico, con un castiIlo fuera de París rodeado de jardines diseñados por Le Nótre, el jardinero de Versalles. Murió en 1682 y poco antes de su muerte le visitó en su casa Luis XIV, que iba a Fontainebleau y se desvió de su ruta sólo con ese fin. Es un gesto muy significativo si tenernos en cuenta el hecho de que los cortesanos que rodeaban a Luis XIV se disputaban la oportunidad de retirar de su habitación el orinal matutino. Fue Rossignol quien inició una tradición de excelente criptofía francesa, que continuaría hasta la época de Napoleón y su famosa y compleja *grand chiffre*, la Gran Clave de París (Urban, 2001).

La invención del telégrafo a mediados del siglo XIX señaló el advenimiento de las comunicaciones basadas en señales. Las señales enviadas a lo largo de la línea telegráfica eran más rápidas y más fidedignas carta enviada por correo, y a finales del siglo XIX el servicio de correos británico podía transmitir cuatrocientas palabras al minuto por los cables que comunicaban Londres con su creciente imperio. La mayoría de estos mensajes se enviaban *en clair*, sin absolutamente ningún cifrado, porque en esa etapa la comunicación telegráfica era aún primordialmente una tecnología británica. Cuando un mensaje salía de Londres hacia Bombay o Hong Kong, sólo se podía interceptar captándolo en los grandes cables tentaculares que se entrecruzaban en el lecho del océano. Y la Marina británica controlaba los mares (West, 1987: 24-26). De todos modos, mientras que podía resultar difícil localizar a un correo determinado y encontrar en su persona el mensaje secreto, las líneas

telegráficas no estaban ocultas. Del telégrafo en adelante, ha sido un axioma de la interceptación de comunicaciones el que las mismas tecnologías que facilitan la comunicación facilitarán también su interceptación. Así, si bien la radio inalámbrica inventada por Guglielmo Marconi a principios del siglo XX liberó al usuario de la pendencia de los cables telegráficos, liberó también de esa limitación al al espía. Marconi puso en marcha la señal libre, enviándola al aire, en el siglo que siguió fue allí donde permaneció. Sólo en los últimos años, con el desarrollo de cables de fibra óptica de alta capacidad, ha empezado a descubrirse que la señal podría volver a la tierra y hacerse más segura en el proceso.

El 16 de enero de 1917, Arthur Zimmermann, ministro de Exteriores de Alemania, envió un telegrama al embajador alemán en Ciudad de México (Tuchman, 1996: 112-115). El telegrama decía "130 13042 13041 8501 115 3528 416..." a lo largo de toda una página, una larga cadena de códigos numéricos. Zimmermann no tenía ningún medio de saber cuando remitió el telegrama que se convertiría en el episodio clave de Sigint de la Primera Guerra Mundial y que sería decisivo para el envío de tropas estadounidenses a Europa. El telegrama anunciaba que Alemania estaba a punto de iniciar una guerra submarina ilimitada y proponía una alianza entre Alemania y México. Animaba también a México "a reconquistar el territorio perdido de Texas, Nuevo México y Arizona".

Los británicos interceptaron el telegrama y los decodificadores de la habitación 40, la Habitación 40, la Cámara Negra de Inglaterra durante la guerra, descifraron el código (Singh, 1999: 112-115). Pero los británicos tenían claro ya uno de los principios básicos del desciframiento de códigos: no permitas nunca que sepan que estás escuchando. Inglaterra llevaba un tiempo intentando arrastrar a Estados Unidos a la guerra y el almirante sir William Hall se dio cuenta de que lo único que tenía que hacer era pasar el telegrama descifrado a los estadounidenses para conseguirlo al fin. Pero vacilaba porque no quería enseñar sus cartas y porque suponía que cuando los alemanes empezasen a torpedear barcos civiles, los estadounidenses, que aún lamentaban la pérdida de los 1.195 pasajeros del Lusitania en 1915, necesitaban poco estímulo más para participar en las hostilidades. Pero el 3 de febrero, dos días después de que el káiser iniciase la guerra naval sin limitaciones, Woodrow Wilson proclamó que Estados Unidos mantendría su neutralidad a pesar de todo.

Incluso en estas circunstancias, Hall se mostraba reacio a pasar el telegrama directamente. En vez de eso, se dio cuenta de que si podía conseguir de algún modo ese mismo telegrama a través de canales humanos en vez de los de Sigint, podría preservar la integridad de su operación interceptora. Así que contactó con un espía británico residente en México, conocido sólo como señor H., que procedió a infiltrase en el servicio de correos mexicano y a robar una copia de una versión revisada y descifrada del mensaje. Esta versión se pasó a los -estadounidenses y a la prensa y en cuestión de días el presidente Wilson proclamaba que el telegrama era una "prueba elocuente" de la ignominia de los alemanes, y en abril Estados Unidos se incorporó al conflicto.

El estatuto de la Habitación 40 lo redactó en I9 I4, en vísperas de la guerra, un joven llamado Winston Churchill (Stafford, 1999: 34). Churchill contrajo a partir de esta temprana experiencia una fascinación por el espionaje de señales a la que tendría ocasión de entregarse plenamente durante la segunda guerra mundial. Aunque tanto Inglaterra como Estados Unidos mantuvieron servicios de desciframiento de códigos durante el periodo de entreguerras, hasta la segunda guerra mundial no empezaron a aproximarse a lo que son hoy sus respectivas operaciones de Sigint, y su cooperación en estas cuestiones. La tecnología y la utilidad de Sigint aumentaron notoriamente durante la segunda guerra mundial. Mientras que el ejército y la marina estadounidenses tenían unos cuatrocientos descodificadores en la primera guerra mundial, en la segunda guerra mundial tenían dieciséis mil (Kahn, 1996: 611). Respecto al valor de este esotérico campo, Churchill escribió en *Their finest hour*:

> Ésa era la guerra secreta, cuyas batallas se perdían y se ganaban sin que el público lo supiese; y que sólo entendían con dificultad, incluso ahora, los no incluidos en los pequeños círculos científicos selectos que participaban en ella. Nunca habían desencadenado una guerra igual hombres mortales. Los términos en los que se podía registrar o en los que se podía hablar de ella eran ininteligibles para la gente ordinaria. Sin embargo, si no hubiésemos controlado su sentido profundo y utilizado sus misterios, incluso cuando sólo los atisbábamos en vislumbres, todos los esfuerzos, todas las proezas de los pilotos de los cazas, la bravura y los sacrificios de la gente habrían sido en vano (Churchill, 1949: 381).

Churchill estuvo pendiente del espionaje de señales durante la guerra e insistió en leer personalmente las transcripciones en bruto de las trascripciones en bruto de las comunicaciones interceptadas

(Stafford, 1999: 223). El personal del número 10 de Downing Street recibía todas las mañanas una caja marcada con la insignia de la reina Victoria. No se permitía abrir la caja a nadie, se llevaba directamente a Churchill, que utilizaba una llave especial que llevaba colgada de un aro a la cintura para abrirla. La caja contenía las comunicaciones del enemigo más recientemente interceptadas, que Churchill denominaba sus "huevos de oro". ("Debo intentar conseguir que mi gallina, que es extremadamente complicada y sumamente sensible, ponga unos cuantos huevos más", escribía a su esposa Clementine en I944). Examinaba los documentos con sir Stewart Menzies, conocido como C, el nombre en clave tradicional del jefe del espionaje británico. Leyendo comunicaciones interceptadas de los italianos y de los japoneses y, a partir de I943, de los alemanes, Churchill pudo tener un conocimiento sin paralelo de la guerra mientras se libraba. Le complacía esta omnisciencia secreta y desarrolló un apetito insaciable por ella, vigilando a países neutrales como Irlanda, Turquía, España, Portugal y la mayoría de las naciones de los Balcanes y de América del Sur (Stafford, 1999: 36-37). Espiaba también a los aliados: a los Franceses libres de De Gaulle, los holandeses, los checos y otros gobiernos en el exilio. Churchill tenía que tener sus huevos de oro incluso cuando viajaba. Cuando fue a entrevistarse con Roosevelt en la costa de Terrranova para la reunión de la Carta Atlántica en el verano de 1941, especificó que debían enviársele las comunicaciones interceptadas en una caja lastrada para que, si el avión era derribado en el mar, los documentos se hundiesen inmediatamente.

El desciframiento de los códigos Enigma alemanes por los sores universitarios y los especialistas en crucigramas de Park se ha convertido, en el último cuarto de siglo, en uno de los aspectos más ampliamente documentados de la segunda guerra mundial. Sin embargo, hasta los años setenta, había poca información asequible al público sobre interceptación y desciframiento de códigos durante la guerra. La cultura del secretismo que había caracterizado por necesidad estas operaciones en época de guerra subsistió en realidad, como un reflejo residual, en el periodo de posguerra. De hecho, hasta I978 no anunció David Owen, entonces ministro de Exteriores del gobierno laborista inglés, que las personas que habían trabajado con el "material de Enigma" durante la guerra podían finalmente admitir que lo habían hecho (West, 1987: 20).

En la primavera de 1941, un pequeño equipo de descodificadores estadounidenses (dos de la marina y dos del ejército) cruzaron el Atlántico (Bamford, 1983: 312). Estaban al mando de un oficial del ejército de la reserva y criptógrafo matemático llamado Abraham Sinkov. Llevaban con ellos un cajón que contenía una reproducción cuidadosamente empaquetada de la máquina codificadora de la diplomacia japonesa conocida como Purple, una pieza de maquinaria pequeña pero pesada que se utilizaba para convertir texto normal en texto codificado. Era un regalo para los descodificadores británicos de Bletchley Park, y los británicos les dieron a los estadounidenses a cambio una colección de equipo criptológico avanzado para que lo utilizasen en su agencia, que tenía el cuartel general en Arlington Hall, un colegio femenino adaptado de Arlington, Virginia. Este episodio fue significativo por una serie de razones. En primer lugar, la máquina Purple se utilizaba para cifrar comunicaciones diplomáticas, y si uno tiene a su disposición los medios de pasar a código una comunicación, puede generalmente operar a la inversa y descubrir cómo descifrar ese código (Stafford, 1999:56). En segundo lugar, en la primavera de 1941 Estados Unidos aún no había entrado en la guerra. Y en tercer lugar, este favor señala el comienzo de una amistad que modificaría el equilibrio del espionaje global y del poder en la guerra fría y después de ella.

Inglaterra había reunido un equipo de brillantes criptógrafos para descifrar los códigos alemanes y japoneses en Bletchley Park. Hasta la decisión de emplazar este centro neurálgico estratégico en medio de los hornos de ladrillos y las instalaciones ferroviarias de un pueblo en decadencia de Buckinghamshire indicaba la tremenda importancia que había adquirido ya Sigint. Una de las razones era que Bletchley Park quedaba aproximadamente entre Oxford y Cambridge, lo que permitiría mejor acceso a matemáticos y descifradores. Pero había otra razón, además: pocos lugares de Inglaterra están más alejados del mar. Los británicos no querían correr el riesgo de que este valor militar, el más estimable y secreto de todos, pudiese caer manos del enemigo en caso de invasión (Stevenson, 1976: 48).

En abril de 1943, después de que los estadounidenses se incorporaran al conflicto, se despachó otra misión a Bletchley Park, dirigida en esta ocasión por William Friedman, el criptoanalista estadounidense más brillante de la época (Smith, 1992: 150-152). Se llamaba en realidad Wolfe Frederick Friedman y había nacido en Rusia y emigrado a Pittsburgh en 1893, cuando aún era un bebé, le había

arrastrado a la criptografía en su juventud primordialmente una muchacha (Elizabeth Smith, que se convertiría en su esposa) que trabajaba en ese campo en los laboratorios Riverbank de Illinois. Friedman había sido oficial criptógrafo en la primera guerra mundial y se convirtió en un especialista en ese arte distinguido e influyente. En el viaje a Inglaterra iban con él el coronel Alfred McCormack, jefe de la nueva rama especial del Servicio de Transmisiones, que había realizado una revisión global de las operaciones estadounidenses de Sigint después de Pearl Harbor, y Telford Taylor, un abogado de treinta y cinco años formado en Harvard que sólo llevaba cinco meses vinculado a la rama especial y a Arlington Hall. Taylor se haría famoso después de la guerra como fiscal jefe en los juicios por crímenes de guerra de Núremberg; es menos conocido el hecho de que durante la mayor guerra fue el principal enlace en Gran Bretaña de la inteligencia de señales estadounidense.

Los tres estadounidenses fueron recibidos calurosamente por sus colegas británicos. Para personas intrigadas por el aspecto intelectual de la criptografía, debía de ser reconfortante poder hablar abiertamente sobre el tema y enterarse de en qué habían estado trabajando "los primos" del otro lado del Atlántico. Lo que descubrió la delegación de Friedman fue que la operación de descifra-miento de códigos británica estaba mucho más desarrollada y era mucho más profesional de lo que ellos habían imaginado. Bletchey Park tenía una nómina de más de cinco mil empleados y los británicos iban muy por delante de los estadounidenses en el desarrollo de las prácticas y los procedimientos de interceptación y descodificación.

Friedman, McCormack y Taylor estaban allí para hacer algo más que simplemente observar. Tras su llegada, empezaron a negociar lo que sería el primer acuerdo escrito importante que vinculó a Inglaterra y a Estados Unidos en la inteligencia de comunicaciones, precursor del que rige hoy la relación. El acuerdo BRUSA, como se le llamó, fue el primer pacto significativo de este género: una alianza sobre Sigint entre dos naciones. El motivo de BRUSA era evitar una duplicación de esfuerzos diferenciando esferas geográficas en las que se centraría cada potencia y coordinar el intercambio de datos confidenciales e información. El texto del acuerdo fue secreto durante medio siglo, pero la NSA acabó haciéndolo asequible al público en 1995. Decía que "Estados Unidos y los británicos acuerdan

intercambiar de forma completa toda información relacionada con la detección, identificación e interceptación de señales y el desciframiento de códigos y cifras utilizados por las fuerzas aéreas y militares de las potencias del Eje"[198]. El acuerdo establecía que Estados Unidos asumiría la responsabilidad de leer las comunicaciones japonesas, mientras que los británicos se centrarían en los alemanes y los italianos. Se acordaba que "toda información secreta asequible descodificada deberá ponerse a disposición de los oficiales de Enlace y si ellos lo consideran necesario se intercambiará entre Londres y Washington". El texto desclasificado contiene aún la admonición: "Parte I que debe ser destruida por el fuego una vez leída". Una vez firmado el acuerdo, Friedman y McCormack volvieron a casa y Taylor se quedó para supervisar personalmente el intercambio de técnicas e información (Smith: 1992: 160-163).

En noviembre de 1943, seis meses después, representantes de treinta países aliados se reunieron en Washington para negociar una colaboración más amplia en la inteligencia de señales (West. 1987: 287). A británicos y estadounidenses se unieron agentes de los servicios de inteligencia de Canadá y Australia, y fue en esta reunión donde los participantes empezaron a desarrollar el embrión de una cooperación internacional más amplia que se formalizaría después de la segunda guerra mundial en el acuerdo UKUSA.

Durante los últimos seis meses de 1945 afloró un número extraordinario de rasgos del paisaje internacional de hoy. El 6 de agosto, la tripulación del *Enola Gay* arrojó la primera bomba atómica en Hiroshima. Tres días después, la tripulación del B-29 conocido como *Bock's Car* arrojó una segunda bomba en Nagasaki. El 2 de septiembre, oficiales japoneses firmaron una rendición incondicional a bordo del acorazado *Missouri*, anclado en la bahía de Tokio. El 24 octubre se fundó Naciones Unidas. Y el 20 de noviembre de 1945 empezaron los juicios de Núremberg, bajo la dirección de Telford Taylor y del fiscal general Robert H. Jackson.

Mientras estos acontecimientos se entronizan en los libros de historia como episodios que definen una época, otro acontecimiento de esos meses, que tuvo una influencia de trascendencia parecida en la forma de actuar de la sociedad internacional en los años siguientes, se ha pasado por alto mayoritariamente. Cuando terminó la

[198] Acuerdo BRUSA del 17 de mayo de 1943, publicado en *Cryptologia* 21, 1, enero de 1997.

guerra con la victoria de los Aliados, debido en no pequeña medida a su cooperación secreta en la inteligencia de señales, éstos decidieron continuar con la alianza en época de paz. El 12 de septiembre de 1945, sólo unos días después de la rendición japonesa, el presidente de Estados Unidos, Harry Truman, firmó un memorándum confidencial de una sola frase que autorizaba al ministro de Guerra y al ministro de Marina "a continuar la colaboración en el campo de la inteligencia de comunicaciones entre el Ejército y la Marina de Estados Unidos y los británicos, y a ampliar, modificar o interrumpir esta colaboración de acuerdo con los intereses de Estados Unidos" (Smith, 1992: 212).

¿Por qué extender esta cooperación íntima al periodo de paz? Parte de la explicación son los temores persistentes de los aliados respecto a la seguridad de posguerra, en relación sobre todo con la Rusia de Stalin. Los estadounidenses estaban preocupados control de las señales que volaban por el mundo era incompleto: sus estaciones de interceptación naval estaban centradas principalmente en el Pacífico, en lugares como Guam, Samoa y Okinawa, y su control del Atlántico se centraba en el sur, en Puerto Rico, Brasil y la zona del Canal de Panamá. Los británicos, por su parte, tenían estaciones de interceptación en el Atlántico norte y la zona del mar del Norte, así como en el Mediterráneo Y en torno al mar Rojo, no indico y el Pacífico sur. Los británicos tenían acceso también a estaciones de interceptación de Canadá, Australia, Nueva Zelanda y Sudáfrica. Debido en parte a que habían compartido la carga durante la guerra, en 1945 Estados Unidos y el Reino Unido poseían cada uno de ellos lo que le faltaba al otro, y sólo a través de la cooperación continuada podían tener ambos el tipo de omnisciencia estratégica global que parecía prudente en un periodo inseguro para ellos (Smith, 1992: 217-225).

Así que, en febrero de 1946, William Friedman fue a Inglaterra para otra ronda de negociaciones. Esta vez las negociaciones duraron casi dos meses, e Inglaterra había sido autorizada por los gobiernos de Ottawa y Canberra a negociar en su nombre. Presidió las negociaciones sir Stewart Menzies. Era un hábil táctico e interrumpía la reunión cuando surgía un asunto particularmente espinoso proponiendo a los participantes que se fueran al Ritz a almorzar. A su regreso a la sala de reuniones, varias botellas de clarete después, solían mostrarse considerablemente más flexibles (Andrew, 195:

162-163).

En estas reuniones se decidió que la oficina de enlace estadounidense instalaría en Londres y que debían introducirse diversos procedimientos para evitar que se duplicasen tareas, un riesgo constante en un entorno de trabajo tan compartimentado y secreto. Se acordó que los dos países compartirían el material procesado y que se establecería un programa de intercambio, que permitiría a los empleados de una agencia pasar varios años trabajando para la otra (Richelson, Ball, 1990: 3).

En el curso de estas negociaciones empezó a tomar forma un documento. En su forma final abarcaba unas veinticinco páginas, pero se mantendría como una elipsis en el registro histórico, un pasaje breve aunque trascendental que simplemente se cortó. Hasta la fecha del documento genera polémica entre los historiadores. El doctor Louis Tordella, legendario criptógrafo de la NSA, confirmó antes de morir al historiador del espionaje británico Christopher Andrew que estuvo presente en la firma y que se produjo en junio de 1948 (Andrew, 1995: 162-163). Tal vez debido a que las negociaciones fueron tan prolongadas y entrañaron sucesivos acuerdos provisionales, se da a menudo como fecha 1947. Estaban también presentes en la firma, según Tordella, un tal coronel Kirby y un tal coronel Hayes del ejército, un tal capitán Roeder de la marina, John Morrison de las fuerzas aéreas, y Benson Buffham y Robert Packard del Departamento de Estado. Y el documento se denominó "Acuerdo de inteligencia de comunicaciones Reino Unido-Estados Unidos, o simplemente, UKUSA".

Pese a la mucha tinta que se ha gastado escribiendo sobre el tema, a que la existencia del acuerdo ha sido reconocida por numerosos antiguos agentes de los servicios de inteligencia y a que dio origen una de las alianzas de esos servicios más coordinadas y duraderas de la historia, el documento aún no es de acceso público y las agencias participantes no han confirmado ni desmentido su existencia. La fase inicial del acuerdo, que se firmó en 1947, vinculó sólo a Estados Unidos y el Reino Unido (Bamford, 2001: 40). El acuerdo disponía que el GCHQ utilizaría sus estaciones de escucha de Inglaterra y de Chipre para controlar Europa occidental y Oriente Próximo. Al año siguiente se incorporaron como "segundas partes" Canadá, Australia y Nueva Zelanda (Richelson, Ball, 1990: 5-6).

En años subsiguientes se incorporó a la alianza un grupo más de

"terceros", como Japón, Corea del Sur y varios aliados de la OTAN. Pero, significativamente, fue un acuerdo escalonado, en modo alguno no entre iguales. Incluso Inglaterra, aunque pudiese haber esta condiciones aproximadas de igualdad durante la guerra, se vio relegada gradualmente a medida que Estados Unidos solidificó su posición como superpotencia durante la guerra fría. Un antiguo agente de la NSA lo expresaba así: "[Toda la] información llega a Estados Unidos, pero Estados Unidos no corresponde del todo pasando información a las otras potencias" (Richelson, Ball, 1990: 8). En realidad, la mayoría de las bases estadounidenses emplazadas en territorio extranjero, incluida RAF Menwith Hill, envían la información directamente a Fort Meade, Maryland, tras lo cual puede distribuirse a otras potencias siguiendo el criterio de lo que "se necesita saber". Aunque Inglaterra alberga la oreja gigante en Menwith Hill, sólo oye lo que Estados Unidos quiere que oiga" (Rufford, 1998).

Los términos del acuerdo son aún menos generosos por lo que se refiere a terceros. Japón, por ejemplo, ha permitido a Estados Unidos construir una docena de instalaciones de escucha en su territorio y situar allí el Cuartel General del Extremo Oriente de la NSA (West, 1987: 287). Sin embargo, desde 1981 la NSA ha encargado a la agencia miembro de Nueva Zelanda, el GCSB, interceptar y controlar cantidades inmensas de tráfico diplomático japonés (JAD, en la taquigrafía del gremio). También es interesante el hecho de que, aproximadamente al mismo tiempo que se firmó el acuerdo UKUSA, se creó la Organización del Tratado del Atlántico Norte, en abril de 1948. Los términos de UKUSA no se vieron afectados por la OTAN. El tratado se limitó a ampliar el territorio en que se podían construir abiertamente nuevas estaciones de escucha (Hager, 1996: 94).

Después de hacer un recorrido por el perímetro de la instalación de la NSA en Menwith Hill y tras contemplar, hipnotizado, aquellas esferas blancas que parecían balancearse ingrávidas en los prados, pensé que aunque el GCHQ no desclasificase el acuerdo UKUSA, podría al menos reconocer su existencia. Después de todo, yo había visto aquella instalación estadounidense gigante en el centro de lnglaterra, había caminado alrededor de ella. ¿ Qué daño podía hacer que se aceptarse lo evidente? "El Reino Unido y Estados Unidos tienen una relación excelente, que nos beneficia a ambos y a la OTAN, en este trabajo en colaboración con fines de defensa común

-me explicó por correo electrónico Bob McNally, un portavoz del GCHQ-. Ha habido una larga tradición de cooperación entre nosotros (…). No hacemos comentarios ni discutimos los detalles de la relación, ni las operaciones de nuestros aliados". Esta respuesta era bastante característica. Nadie niega que haya una amistad, incluso una "relación especial". Pero cualquier intento de ir más allá de esos comentarios lisonjeros está condenado al fracaso. De todos modos, aunque los funcionarios no reconozcan la alianza por su nombre, deslizan y transmiten de vez en cuando detalles relevantes. En octubre de 2002, la primera ministra de Nueva Zelanda, Helen Clark, explicó a *The New Zealand Herald* que su país aún formaba parte de algo que denominó "el mejor club de inteligencia". Cuando le preguntaron más sobre ese club en la televisión del país, Clark dijo que Nueva Zelanda era un "miembro fundador" del club, "junto con Estados Unidos, Inglaterra, Australia y Canadá" (Young, 2002).

Un día de 1970 salió un camión de la sede central de la empresa aeroespacial TRW, en Redondo Beach (California). Transportaba un satélite geoestacionario, una pieza de la tecnología del espionaje que iba a revolucionar la forma de interceptar señales de Estados Unidos y a aproximar entre sí más que nunca a las cinco naciones de la alianza UKUSA. "Geoestacionario" significa simplemente que el satélite orbita en sincronía con la rotación de la tierra, de manera que se mantiene siempre sobre el mismo punto. Cuatro años antes, TRW ha recibido el encargo de la CIA de fabricar cuatro de esos satélites, debían lanzarse al espacio a principios de los años setenta. Éste era primer satélite del programa, que se llamaba en clave *Rhyolite* y pasaría a conocerse entre la gente que lo manejaba desde tierra como *Bird* (Ball, 1988, Lindsey, 1979)[199].

Como construir satélites es tan caro, *Bird I* debía realizar todo una serie de funciones. Su tarea primordial sería la telemetría: ondas de radio y cambios atmosféricos para detectar pruebas de misiles. Pero otra de sus funciones era interceptar señales de comunicaciones. Debido a la curvatura de la Tierra, cuando envías una señal de radio entre torres repetidoras que están a cierta distancia, parte

[199] Ball (1988, caps. 2-4) y Lindsey (1979, cap. 9). William Burrows indica que este primer modelo fue una "versión operativa experimental", a la que siguió con el tiempo el primer Rhyolite Bird "plenamente operativo" en 1973. William Burrows, *Deep black: space espionaje and national security* (1986: 191).

esa señal seguirá en línea recta, más allá de la torre, perdiéndose espacio. A esto se le llama derrame microondular. La calidad señal se va deteriorando a medida que va alejándose de la Tierra, pero el mensaje seguirá siendo discernible a treinta mil kilómetros de ella, donde está previsto que estén situados los satélites *Rhyolite.* Por tanto, en palabras de Robert Lindsey, el reportero de *The New York Times* que fue una de las primeras personas que escribieron sobre el programa, estos satélites "podían controlar el tráfico comunista en gran parte de la masa continental europea, escuchando a un comisario soviético hablar desde Moscú con su amante de Yalta o a un general hablando a sus lugartenientes de un lado a otro del gran continente" (Lindsey, 1979: 57). James Bamford, que con dos densos libros sobre la de la NSA es la autoridad civil indiscutible sobre la agencia, se refiere a *Rhyolite* como "el primer verdadero puesto de escucha de la NSA en el espacio" (Bamford, 2001: 367-368).

Bird I, envasado en un gran contenedor a bordo del camión, fue transportado a Cabo Cañaveral (Florida), donde se lanzó desde un vehículo lanzador Atlas-Agena D (Bamford, 2001: 368). *Bird I* era un cilindro achaparrado, de metro y medio de longitud y unos tres cuartos de tonelada de peso, que estaba diseñado para desplegarse en el espacio en forma de un paraguas gigante, con un disco de poco fondo y de veintiún metros de anchura, de cuyo centro salía una larga antena (Burrows, 1986: 193). El disco estaba provisto de dos largas alas de células de silicona, que podían convertir la luz en energía. Y el artefacto llevaba incrustadas dos docenas de receptores microondulares. Lo más probable es que el satélite pasase varios meses sobre Estados Unidos, mientras los técnicos de laboratorio afinaban y calibraban sus delicadas piezas. Luego inició su migración a un punto situado sobre el Ecuador, cerca de Indonesia y Australia... el punto más estratégico para recoger señales de la Unión Soviética y de China.

Rhyolite era completamente independiente de los puestos de escucha de la variedad terrestre y, al mismo tiempo que se ponía a punto *BiTd I* para su lanzamiento desde Estados Unidos, había otros preparativos en marcha al otro lado del planeta. En el sofocante corazón da Centro Rojo de Australia, a unos diecinueve kilómetros de la población de Alice Springs, estaban pasando cosas extrañas. El Centro Rojo es una extensión árida de arena color herrumbre y matas de espinifex, la hierba seca que es una de las pocas cosas que

pueden crecer en unas condiciones de desierto tan duras. Alice, como le llaman los locales, es el único puesto destacado en centenares de kilómetros, una mota polvorienta e inhóspita en el centro mismo de la masa continental australiana. En los años sesenta, Alice era una pequeña comunidad de unos cuantos miles de blancos, principalmente recios rancheros a los que les gusta el aislamiento, y varios miles de aborígenes, cuyos ascendientes llevaban milenios viviendo en la zona. Así que a los locales debió de parecerles sumamente extraño que, tres años antes del lanzamiento del *Bird I*, una empresa con sede en Texas llamada Collins Radio Co. instalase una oficina en la población[200].

Más sorprendente incluso que el hecho de que estos estadounidense se adentrasen en el corazón del interior de Australia y fuesen capaces de aguantar temperaturas de 46^0C era el hecho de que planeasen quedarse. Collins estaba allí para ayudar a construir una base al lado de la población, en una cuenca poco profunda entre afloramientos al pie de las montañas Macdonnell. La base sólo contenía inicialmente dos radomos, que ocultaban antenas parabólicas de 33 y 21 metros de diámetro, respectivamente. Estos dos radomos se instalaron en 1968, pero les siguieron a lo largo de los años otros doce, que elevaron a catorce el número de radomos que hay hoy allí. A los radomos se incorporaron una docena de antenas más y unos veinte edificios de apoyo de una sola planta, entre los que se incluye una enorme sala de ordenadores de unos quinientos cincuenta metros cuadrados, que se dice que es una de las mayores del mundo. Collins aportó gran parte de la infraestructura básica, IBM fue el principal contratista por la estación y otra empresa de Texas, E-Systems, corrió con la responsabilidad del manejo y dirección de la sala de ordenadores. Así que, si bien el nombre oficial, aunque críptico, de la estación era Base de Investigación Espacial de la Defensa Conjunta, era aún en gran parte una operación estadounidense. El nombre esta cabeza de playa del sistema de interceptación de UKUSA en Australia es Pine Gap.

Es difícil transmitir hasta qué punto está aislado Pine Gap. La está literalmente en medio de la nada. Se encuentra en la extensión más remota del continente más remoto de la tierra. Un antiguo técnico de E-Systems que pasó varios años allí me explicó que después de un corto espacio de tiempo los jóvenes estadounidenses enloquec-

[200] Detalles tomados de Ball, *Pine Gap*.(1988).

ían y se entregaban progresivamente a arrebatos báquicos de excesos, bebiendo y copulando descontroladamente a falta de otra cosa mejor que hacer. Por supuesto, la localización es remota a posta (Ball, 1988: 90). Cuando se concibió en los años sesenta la idea de utilizar satélites geoestacionarios para la inteligencia de señales, la principal preocupación al elegir emplazamientos para las estaciones terrestres era que los soviéticos no pudiesen interceptar de ninguna manera los enlaces descendentes. Los estadounidenses necesitaban, para mantener los satélites en órbita de aparcamiento sobre el océano Índico, instalar un enlace descendente en el hemisferio sur, ya que la curvatura de la Tierra impide a los satélites transmitir desde allí directamente a Estados Unidos. El enlace descendente no podía instalarse en una isla como Diego García o Guam, porque sería vulnerable a las naves Sigint soviéticas que buscaban señales al lado de la costa. Aunque este tipo de operación era siempre azarosa, en esta ocasión el riesgo era aún mayor porque, con el fin de mantener al *Bird* I ligero de peso y fácil de propulsar, los arquitectos habían decidido ponerlo en órbita sin ningún sistema de cifrado a bordo. Los mensajes que transmitía a la Tierra se enviaban en lenguaje natural, es decir, sin ninguna codificación (Bamford, 2001: 368).

Considerando todo esto, Pine Gap era una solución ideal. Los dieciocho kilómetros cuadrados del entorno de la base están protegidos como una zona de barrera para reducir cualquier tipo de interferencia o electrónica (Ball, 1988: 90-91). Los arrendatarios de los pastos que rodean la estación impiden el acceso a los visitantes. No sería posible, pues, instalar un tipo de antena que recibiese señales de satélite en ninguna parte en un radio de unos ochenta kilómetros. Los controladores del tráfico aéreo del aeropuerto de Alice Springs informan de cualquier vuelo sospechoso, así que hay pocas posibilidades de interceptación por sobrevuelo. Y el lugar está a centenares de kilómetros del mar, así que no hay peligro de que barcos soviéticos capten las señales del *Bird I*.

Como el proyecto de Pine Gap ha sido siempre un proyecto reservado, se han hecho muy pocos comentarios oficiales sobre sus operaciones o capacidades. El acuerdo para crear la base lo firmaron los gobiernos de Australia y de Estados Unidos el 9 de diciembre de 1966 y dice que se dedicará a “la investigación espacial conjunta”. Sin embargo, el acuerdo identificaba a la agencia estadounidense

responsable de la base como Agencia de Proyectos de Investigación Avanzada, o ARPA (en sus siglas inglesas), que hoy se conoce como DARPA (una enmienda del acuerdo reemplazó en 1977 esta referencia por otra más genérica, que decía que supervisaría la estación el Ministerio de Defensa). Las veces que se ha reconocido la mera existencia de la estación se ha afirmado invariablemente que la base se dedica a la investigación espacial o a "la verificación del control de armamento" (Ball, 1988: apéndice, 1,2). Pocos dudan que la estación fue un medio importante de controlar las actividades de investigación nuclear y las pruebas nucleares de los soviéticos y de otras potencias a través de diversas formas de telemetría satelital. El ministro de Asuntos Exteriores australiano Bill Hayden comentó una vez que "es sumamente improbable que se hubiese llegado a firmar un solo acuerdo importante de control de armamento entre las superpotencias si no hubiese existido Pine Gap" (Ball, 1988: 92). Pero incluso en punto culminante de la guerra fría, en la década de los ochenta, Desmond Ball, profesor de la Universidad Nacional de Australiana y el especialista más sobresaliente en inteligencia de señales del país, calculaba que el programa estadounidense de satélites estacionarios dedicaba al control de armas menos del 40 % de los recursos y esfuerzos (Ball, 1988: 92). Además, como Ball deja claro, el programa que inició el *Bird I* llevaba funcionando algunos años cuando se lanzó el primersatélite *Rhyolite* en 1970; en realidad precedió a todos los tratados y discusiones serias entre estadounidenses y soviéticos sobre control de armamento. Según Ball, los técnicos de la Sección de Análisis de Señales de Pine Gap podían escuchar comunicaciones desde el principio y algunos pasaron por la experiencia inquietante, durante los últimos años de la guerra de Vietnam, de escuchar los gritos radiados de infantes de Marina estadounidenses heridos que pedían ayuda (Ball, 1988: 53).

Pero ¿qué hace hoy Pine Gap? Podía esperarse que la base se hubiese cerrado después de la guerra fría. Otra base estadounidense situada varios centenares de kilómetros al sur, con el lírico nombre de Nurrungar (que se deriva, muy adecuadamente, de la palabra aborigen que significa "escuchar"), se cerró en 2000, Y muchos de sus empleados y gran parte del equipamiento se trasladaron a Pine Gap. Al mismo tiempo, las autoridades australianas anunciaron en el verano de I998 que el acuerdo de Pine Gap se había renovado por otros diez años.

Hoy la base tiene casi novecientos empleados, aproximadamente la mitad australianos y la mitad estadounidenses ()[201]. Ha habido conflictos laborales en el pasado, haciendo huelga los australianos porque les pagan menos que a sus colegas estadounidenses, pero por lo demás las relaciones son bastante cordiales. Alice Springs está actualmente lleno de estadounidenses. Nunca hablan de su trabajo, por supuesto, pero participan en numerosas actividades: ligas de béisbol, clubes de rotarios, la Asociación Mantenga Bello Alice Springs. Y aportan mucho dinero a la economía local[202].

Aunque Bamford se refiere a Pine Gap como el primer puesto de escucha de la NSA en el espacio, la base la dirige en realidad la CIA, que se coordina con la NSA y con la Oficina Nacional de Reconocimiento (NRO, según las siglas en inglés), la agencia responsable del diseño y el desarrollo de los satélites estadounidenses. Pine Gap sólo era en principio una estación repetidora. Recibía señales no cifradas del satélite *Rhyolite*, las codificaba y luego las enviaba a Estados Unidos, bien a TRW o directamente a Fort Meade (Bamford, 2001: 368). Pero Ron Huisken, un australiano que fue jefe de la base desde 1995 a 2001, afirma que Pine Gap ha duplicado su tamaño desde la guerra del Golfo[203]. Lo más probable es que esto refleje hasta qué punto la cobertura del hemisferio sur proporcionada por la base ha ido haciéndose cada vez más vital para las consideraciones estratégicas estadounidenses. Refleja también lo estrechas que son las relaciones entre las comunidades de los servicios de inteligencia de Australia y de Estados Unidos derivadas del acuerdo UKUSA. Hoy Pine Gap es la base de la CIA más grande del mundo. Pero es sólo una de las docenas de bases dirigidas por los servicios de inteligencia y el ejército de Estados Unidos sólo en Australia (Ball, 1980).

La presencia de tantas bases estadounidenses en Australia ha dado origen, a lo largo de los años, a esporádicas controversias. Aún siguen organizándose hoy protestas en torno a varias de ellas, sobre todo en torno a Pine Gap. Cuando sucede esto, las carreteras que

[201] "Aussie War Spies Go on Strike", *Northern territory news,* Australia, 18 de marzo de 2003.
[202] "A Yankee Spy Base in the Outback", *U.S. News and World Report,* 20 de junio de 1983.
[203] "Exofficial Speaks on Role of Australian-US. Pine Gap Monitoring Station", BBC Monitoring International Reports, 13 de marzo de 2003.

llevan a la base se bloquean y quedan bajo control de la policía militar. La polémica de este género de mayor envergadura fue la que se produjo en el otoño de 1975. Había mucha preocupación por entonces en Australia por la presencia allí de bases que formaban parte de la telemetría nuclear estadounidense y podían, por ello, convertirse en objetivos de un ataque nuclear. Aunque todo esto parezca hoy alarmista, conviene recordar la atmósfera general de la guerra fría, en la que estos hechos parecían muy plausibles y, para muchos, inevitables. En el otoño de 1975 se estaba haciendo pública nueva información sobre el papel de la CIA en Australia, lo que avivaba las llamas del debate. En la vanguardia de la crítica de las instalaciones estadounidenses figuraba el primer ministro Gough Whitlam. A finales de octubre, su gobierno laborista reveló que las bases no habían sido supervisadas por el Ministerio de Defensa de Estados Unidos, como se había sostenido anteriormente, sino en realidad por un agente de la CIA, cuye nombre se hizo público. El partido laborista inició investigaciones y se reveló que ni siquiera los altos cargos del Ministerio de Exteriores australiano sabían qué se hacía exactamente en bases como Pine Gap (Lindsey, 1979: 140-141).

El 10 de noviembre, la Organización de Inteligencia de Seguridad australiana recibió un mensaje de su enlace con la ClA que decía que los funcionarios de la agencia estaban sumamente preocupados por el peligro de cualquier posterior revelación sobre la base.

> La CIA está perpleja por lo que significa todo esto, ¿significa algún cambio en nuestro campo de la inteligencia de seguridad bilateral? La CIA no cree que este diálogo con alusiones insistentes a la CIA pueda hacer otra cosa que levantar la tapa de las instalaciones que hay en Australia, donde las personas afectadas han estado trabajando y que son vitales tanto para nuestros servicios como para nuestros países, sobre todo las instalaciones de Alice Springs (Lindsey, 1979: 141).

Se trataba de una cuestión de la máxima importancia para Estados Unidos. El Consejo Nacional de Seguridad consideraba las bases Australia un elemento indispensable para la supervivencia nuclear estadounidense, y se sugería al final del mensaje que si continuaban las revelaciones Estados Unidos podría dejar de dar a Australia acceso privilegiado a la información secreta que obtenían las bases.

Pero Whitlam perseveró. No era aquélla una época buena para estar asociado con la CIA (Lindsey, 1979: 142). Estaban empezando a aflorar revelaciones sobre la participación de la agencia en el de-

rrocamiento de Salvador Allende en Chile, y Whitlam estaba convencido de que había una intromisión similar en los asuntos políticos internos de Australia. Había empezado a decir públicamente que la CIA había canalizado fondos para los partidos liberal y nacional, que se oponían ambos a los laboristas y que apoyaban la presencia de bases estadounidenses . Tenía previsto pronunciar otro discurso sobre el tema el 11 de noviembre, pero no pudo hacerlo porque el general gobernador John Kerr le depuso del cargo.

En el tiempo transcurrido desde entonces, han persistido en Australia diversas teorías sobre la participación de la CIA en este golpe, pero la destitución de Whitlam fue en última instancia un pequeño tropiezo en lo que ha sido por lo demás una historia de amigable cooperación. Aunque inicialmente los empleados australianos de Pine Gap estaban excluidos de la Sección de Análisis de Señales de la base y no tenían acceso en consecuencia a las valiosas informaciones secretas que allí se recogían, en I980 se eliminó la segregación en el complejo y hoy la relación bajo UKUSA es más estrecha que nunca (Ball, 1999). Los directores de las cinco agencias aliadas se reúnen todos los años para planificar y coordinar. Las reuniones son rutinarias y rutinariamente secretas (Hager, 1996: 22). El público no sabe qué país está haciendo de anfitrión qué año ni cuándo se celebran las reuniones. Y la cooperación entre los países de UKUSA no se limita ni mucho menos a la procede del acuerdo secreto. Hay numerosos acuerdos multilaterales y bilaterales más que rigen el intercambio de información secreta entre los países, por no hablar ya de las innumerables convenciones informales que surgen de la cooperación continuada, que son a menudo tan importantes o más que los propios acuerdos escritos (Richelson, Ball, 1990: 135).

En 1999 Bill Blick, general inspector de los servicios de inteligencia de Australia, fue el primer funcionario de un país de la UKUSA que reconoció esta estrecha relación y la red de Sigint que mantienen los países signatarios. “Como es de suponer, hay una gran cantidad de comunicaciones de radio flotando en la atmósfera -explicó a la BBC-, y servicios como el DSD recogen esas comunicaciones en interés de la seguridad nacional”. Cuando le preguntaron si estas informaciones interceptadas se pasaban a Inglaterra y a Estados Unidos, Blick confirmó que “podría ser en ciertas circunstancias” (Bomford, 1999).

Menwith Hill y Pine Gap son sólo dos de las muchísimas bases que

cubren el planeta. Su tamaño y su importancia dan testimonio del alcance del sistema que puso en marcha el acuerdo UKUSA hace más de cincuenta años y de lo estrechamente implicados que están hoy los cuatro signatarios no estadounidenses de ese acuerdo en el espionaje estadounidense. Constituyen, por derecho propio, un mero indicio de los tremendos recursos y las ingentes inversiones que se han dedicado a la red y no hacen más que insinuar las capacidades de ésta. Gough Whitlam infravaloró la importancia que tenía para los gobiernos de los países involucrados que el acuerdo gozase de buena salud y la facilidad con que una alianza entre los servicios secretos podía manipular las necesidades y las demandas de los políticos y los ciudadanos locales. Infravaloró también hasta dónde estarían dispuestos a llegar esos servicios secretos para mantener vigilados todo el asunto político. Una joven empleada del GCHQ cometería un error de cálculo similar un cuarto de siglo después.

Bibliografía

Andrew, Christopher (1995) *Fort he president's eyes only,* HarperCollins, Nueva York, 429.

Baer, Robert (2002) *See no evil,* Crown, Nueva York, XVII.

Ball, Desmond (1988) *Pine Gap,* Allen and unwin, Sidney, caps. 2-4.

- (1980) *A suitable piece of real estate: american installations in Australia,* Hale and iremonger, Sidney.

Bamford, James (2001) *Body of secrets,* Doubleday, Nueva York, 482.

- (1983) *The puzle palace,* Penguin, Nueva York, 312.

Blackstone, William (1979) *Commentaries on the Laws of England,* University of Chicago Press, vol. 4: 169.

Blazar, Ernest (1998) "Inside the ring", *The Washington Times,* 24 agosto.

Bomford, Andrew (1999) "Echelon Spy Network Revealed", *BBC News,* 3 noviembre.

[BRUSA] (1997) ["Acuerdo BRUSA del 17 de mayo de 1943"], *Cryptologia* 21, 1, enero.

Burrows, William (1986) *Deep black: space espionaje and national security,* Rndom House, Nueva York, 191.

Campbell, Duncan (1999) *Interception capabilities 2000,* http://www.iptvreports.mcmail.com/interception_capabilities_-

2000.htm.
Celona, Larry, Hunter, Bread (2003) "Target: Subway", *New York Post,* 9 de febrero de 2003.
Coll, Steve (2004) *GhostWars,* The Penguin Press, Nueva York.
- (2002) "A secret hunt unravels in Afganistan", *The Washington Post,* 24 febrero.
Comisión Nacional (Commission report) sobre ataques terroristas a los Estados Unidos (2004) *The 9/11 report: final report of the national commisssion on terrorist attacks upon the United States,* W.W. Norton, Nueva York, 353.
Conrad, Joseph (1967) *Heart of darkness*, cfr. Alfred A. Knopf, Nueva York, [1902], 9.
Churchill, Winston (1949) *Their finest hour,* Houghton Mifflin, Boston, 381.
Federación de Científicos Estadounidenses (FAS) (s/F) "Intelligence agency budgets", http://www,fas,org.
- (2002) "Time for a rethink", *The economist,* 18 abril.
Gerecht, Reuel Marc (2001) "The counterterrorist myth", *Atlantic Mounthly,* julio/agosto.
Graham, Bob, Nussbaum, Jeff (2004) *Intelligence Matters,* Random House, Nueva York, 86.
Hager, Nicky (1996) *Secret power,* Craig Potton, Nelson (Nueva Zelanda), 40.
Heródoto (1987) *The history,* University of Chicago Press, Chicago, 5: 35.
Horton, Murray (s/f) "Government still coy about UKUSA agreement", *Peaceresearcher,* http:www.converge.org.nz/abc/pr27-79.htm.
Huisken, Ron (2003) "Exofficial Speaks on Role of Australian-US. Pine Gap Monitoring Station", *BBC Monitoring International Reports*, 13 marzo.
Jehl, Douglas (2004) "Abundance of caution and years of budgest cuts are seen to limit CIA", *The New Tork times,* 11 mayo.
Kahn, David (1996) *The codebreakers,* Scribner, Nueva York, 677-689.
Lindsey, Robert (1979) *The falcon and the Snowman,* Simon and Schuster, Nueva York, cap. 9.
Mark Weiser, Mark (1991) "The computer for the twenty-first century", *Scientific American,* septiembre.
Northern territory news (2003) "Aussie War Spies Go on Strike",

Northern territory news, Australia, 18 marzo.
Pasternak, Douglas (2003) "Lack of intelligence", *US News and world report*, 11 agosto.

Pincus, Walter (2002) "The Reasons Behind a White House Rebuke", *The Washington Post,* 24 junio.
- (1998) "CIA's espionaje capability found lacking", *The Washington Post,* 10 mayo.
Rashbaum, William (2003) "Police are focusing more on protecting the subways", *The New York Times,* 14 febrero.
Richelson, Jeffrey, Ball, Desmond (1990) *The that bind,* 2 edc., Unwin and Hyman, Boston, 3.
Risen, James (2003)"US increased alert on evidence qaeda was planning 2 attacks", *The New York Time,* 14 febrero.
- (2004) "Slow-down in chatter", Worries officials, *CNN*, 6 agosto.
Robertson, Geoffrey (1998) *The justice game,* Chatto and Windus, Londres, 125.
Rufford, Nicholas (1998) "Spy Station f83", *The Sunday Times,* 1 junio.
Scheuer, Michael (2004) *Imperial hubris,* Brassey's, Dulles (Virginia), 192-200.
Scott, Bárbara E. (1991) [Fort Meade], *NSA Newslatter.*
Singh, Simon (1999) *The code book,* Doubleday, Nueva York, 15.
Smith, Brandley F. (1992) *The ultra-magic deals and the most secret special relationship,* 1940-1946, Presidio Press, Novato (California), 150-152.
Stafford, David (1999) *Roosevelt and churchil: men of secrets, Overlook Press, Nueva York,* 34.
Stevenson, William (1976) *A man called intrepid,* Harcourt Brace Jovanovich, Nueva York, 48.
Tuchman, Bárbara (1996) *The zimmermann telegram,* Macmillan, Nueva York.
Urban, Mark (2001) *The man who broks Napoleon's codes,* Faber and Faber, Londres.
West, Nigel (1987) GCHQ, Hodder and Stoughton, Londres, 24-26
Woodward, Bob (2004) *Plan of attack,* Simon and Schuster, Nueva York, 213.
Young, Audrey (2002) "PM backs CIA over warnings", *New Zealand herald,* 17 octubre.