Huawei se enfrenta a la historia: Las grandes potencias y los riesgos de las telecomunicaciones, 1840-2021

Rush Doshi y Kevin McGuiness

Brookings Institution, marzo del 2021

Resumen ejecutivo

A finales del 2018, en medio de las preocupaciones estadounidenses de si Canadá acogería a Huawei en sus redes de telecomunicaciones, el primer ministro de Canadá, Justin Trudeau, realizó una serie de declaraciones que reflejaban la sabiduría convencional en gran parte del mundo. "No debería ser una decisión política" declaró en ese momento y aseveró que Canadá no dejaría que "la política interfiriera en las decisiones" sobre el papel de Huawei en su red.[1]

La idea de que la política del poder se pudiera excluir de las cuestiones de las telecomunicaciones no solo era optimista, sino también estaba desconectada de la historia de las telecomunicaciones. Este informe explora esa historia y muestra cómo el poder y las telecomunicaciones casi siempre han estado estrechamente vinculados. Cuando los estados han ignorado esos vínculos y han pasado por alto la seguridad de sus propias redes, los resultados han sido desfavorables y, en ocasiones, desastrosos.

En este informe, se examinan varios casos importantes de competencia entre grandes potencias sobre las telecomunicaciones que datan del comienzo de las telecomunicaciones eléctricas en la década de 1840. Estos casos demuestran que muchas de las cuestiones a las que se enfrentan los legisladores hoy en día son muy similares a otras que han existido en el pasado. Si bien el debate actual sobre la seguridad de la red y la infraestructura 5G puede parecer nuevo, se asemeja, de hecho, a disputas olvidadas que se remontan a los inicios de las telecomunicaciones eléctricas hace unos 150 años. Además, muchos de los elementos comunes de la competencia de las telecomunicaciones en la actualidad, como el uso de organismos normativos, los subsidios estatales, la interceptación de cables, las guerras de información, el desarrollo de mercados nacionales y el cifrado para ganar ventaja, se desarrollaron hace más de un siglo, con importantes lecciones para los debates actuales.

A continuación, se proporciona una lista de estas lecciones clave:

1. **El control sobre las redes globales de telecomunicaciones es una forma de poder político.** Se espera que las redes 5G formen la base de una economía más inteligente y conectada, que conecte un sinnúmero de dispositivos y sensores. Ansiosa por crear estas redes en todo el mundo, China ha subsidiado a sus empresas y proyectos campeones de 5G en todo el mundo como parte de una iniciativa de la “Ruta de la Seda Digital”. Este esfuerzo es análogo a la búsqueda del dominio de las redes por parte de Gran Bretaña en los inicios de la telegrafía eléctrica. Gran Bretaña obtuvo su ventaja durante seis décadas aumentando constantemente la dependencia de otros estados de sus redes, incluso

renunciando a tarifas y beneficios económicos con el fin de atraerlos a tender cables a través de Gran Bretaña, a la vez que reducía la dependencia británica de redes extranjeras. Con el tiempo, controló más de la mitad del tráfico de cables del mundo, la red de radio más extensa y la mayor flota de barcos de tendido de cables. La "hegemonía de la información" de Gran Bretaña le permitió aislar a Alemania de prácticamente todas las telecomunicaciones mundiales en la Primera Guerra Mundial y obligó a Berlín a comunicarse a través de líneas de propiedad británica, susceptibles de monitoreo británico, lo que, posteriormente, demostró ser decisivo en la derrota de Alemania en el conflicto.

2. **Los largos períodos de paz y prosperidad generalmente conducen a la complacencia sobre los riesgos de las telecomunicaciones.** En los últimos 30 años, la paz después de la Guerra Fría y la globalización económica coincidieron con un rápido progreso en las telecomunicaciones, que llevó a los estados a priorizar los beneficios comerciales revolucionarios por sobre los riesgos políticos y de seguridad, incluso permitiendo que sus redes fueran de propiedad extranjera u operadas por extranjeros. Algo similar ocurrió en los inicios de las telecomunicaciones en la década de 1840, que también coincidió con un período de relativa paz y globalización que continuó hasta la Primera Guerra Mundial. Durante gran parte de esa era, el deseo de apropiarse del aparentemente milagroso potencial comercial de las nuevas tecnologías de comunicaciones relegó a un segundo plano cuestiones relacionadas con la confianza en redes o empresas extranjeras. Gran Bretaña se benefició de la complacencia de otros estados creando y, a continuación, aprovechando una posición nodal invulnerable en las redes globales, en que la mayoría de las demás grandes potencias dependían de sus redes.

3. **Cuando los estados se sienten conformes con la seguridad de sus telecomunicaciones, los resultados pueden ser desastrosos y reordenar la política mundial.** Décadas de complacencia alemana sobre su dependencia de las líneas de telecomunicaciones británicas significaron que, para el momento en que Berlín se dio cuenta de los riesgos de dicha dependencia, ya era demasiado tarde para cambiarla. Cuando estalló la Primera Guerra Mundial, Gran Bretaña cortó todos los cables de Alemania y obligó a Berlín a comunicarse a través de redes británicas, con todo el riesgo de interceptación que esto implicaba, lo que provocó el descubrimiento del "telegrama Zimmermann", que contribuyó a que Estados Unidos entrara en la guerra. Del mismo modo, la indisciplina rusa en las transmisiones de radio inalámbricas en la Primera Guerra Mundial permitió que los alemanes interceptaran comunicaciones, "vieran" el movimiento de las tropas rusas en tiempo real y les propinaran una derrota decisiva en la Batalla de Tannenberg. Después, en la Segunda Guerra Mundial, la confianza excesiva de los nazis en sus claves los llevó a realizar pocos esfuerzos para actualizarlas, lo que permitió a Gran Bretaña descifrar los códigos y obtener información que se cree que acortó la guerra dos o cuatro años. Dado el poder de la información, incluso los momentos ocasionales de indisciplina o complacencia de las señales pueden alterar la historia.

4. **La nueva tecnología siempre lleva a nuevos esfuerzos para interceptarla.** La aparición de cables submarinos llevó a esfuerzos para cortar dichas líneas e interferirlas

ya en la guerra Hispano-Estadounidense; las transmisiones de radio dieron lugar a esfuerzos por parte de los rivales de capturar nodos de redes e interceptar transmisiones; y la aparición de claves sofisticadas de cifrado llevó a esfuerzos de escala industrial por descifrarlas. En todas las épocas, algunas personas pensaban que un nuevo avance en las comunicaciones las haría menos vulnerables que las que precedían. Sin embargo, el ciclo de innovación y aprovechamiento siempre continuaba.

5. **Las redes de telecomunicaciones nunca han sido políticamente neutrales, especialmente en tiempos de tensión.** En el 2019, los ejecutivos de Huawei asumieron el compromiso de "sin puerta trasera, sin espionaje", prometieron que su empresa se mantendría al margen de la política y el Gobierno de China se comprometió a respetar este compromiso. Pero ya hace más de un siglo, las empresas de telecomunicaciones y los gobiernos de sus respectivos países hacían públicamente promesas similares mientras, en privado, las rompían y trabajaban juntos en tiempos de paz y de guerra. Por ejemplo, el dominio británico en cables submarinos llevó a los franceses, alemanes y estadounidenses a promover que dichas líneas se mantuvieran neutrales, incluso en caso de guerra. Las empresas británicas declaraban públicamente su neutralidad, pero, en realidad, obedecían los intereses políticos británicos, en especial en momentos de gran tensión, y abandonaron su neutralidad completamente durante los períodos de guerra. El poder que proviene de la interrupción o la interceptación de los flujos de información de los rivales generalmente es demasiado atractivo para que se cumplan, incluso, afirmaciones sinceras de neutralidad.

6. **Los estados, a menudo, buscan a sus propios campeones de telecomunicaciones una vez que reconocen la vulnerabilidad de confiar en las empresas de un competidor o adversario.** Actualmente, Estados Unidos carece de un fabricante importante de estaciones de base 5G, lo que ha suscitado debates sobre si deberían invertir en sus propias empresas o confiar en empresas aliadas. Esto también ha generado desacuerdos sobre hasta qué punto Huawei es, en sí mismo, un campeón estatal de facto. Estos debates tienen algunos antecedentes. A principios del siglo XX, muchos estados dependientes de otros para sus equipos de telecomunicaciones o redes comenzaron a construir sus propios sistemas. Por ejemplo, Alemania fusionó dos empresas alemanas que competían por desarrollos radiales (Siemens & Halske y AEG) para establecer una alternativa alemana al dominio británico en la radio. Muchos otros estados líderes respaldaron a empresas que, aunque ostensiblemente privadas, estaban entrelazadas con los estados que las apoyaban.

7. **La lucha por los estándares de las telecomunicaciones puede determinar qué estados harán uso del poder de la red y, a menudo, esto exige reclutar aliados y socios.** Los estados cuyas tecnologías se convierten en el estándar dominante pueden ejercer poder sobre otros estados. La competencia actual sobre los estándares de la tecnología de las comunicaciones de la información es, de esta manera, similar a la competencia angloalemana por las redes de radio. Gran Bretaña, a través de la Marconi Company, a la cual apoyaba, era tan dominante en comunicaciones radiales inalámbricas que todas las demás grandes potencias tenían que transmitir sus mensajes a través de la red inalámbrica británica, que se negaba a participar con cualquier otra estación inalámbrica. Alemania,

finalmente, consiguió romper dicho dominio a través de un organismo normativo que prohibió esta política de "no intercomunicación" con la ayuda de otras potencias, incluidos Estados Unidos y Francia, una demostración de cómo los enfoques de coaliciones similares hoy en día pueden servirles a los estados liberales para establecer o mantener estándares de tecnología de la información y las comunicaciones (ICT, del inglés *Information and Communications Technology*) si trabajan juntos.

8. **A medida que sus comunicaciones se vuelven más fáciles de interceptar, los estados se vuelcan al cifrado, pero este, a menudo, tiene límites, debido a la persistencia de los adversarios o a los errores de usuario.** Algunas personas afirman que la ansiedad sobre el papel de Huawei en las redes o sobre la vulnerabilidad general de los dispositivos conectados a Internet se mitiga gracias al cifrado moderno. Estos tipos de argumentos tienen un largo historial. En los inicios de las telecomunicaciones, hace un siglo, la posibilidad de que otras personas que controlaran los nodos de las redes pudieran leer los mensajes telegráficos, o de que las transmisiones radiales se pudieran interceptar mediante equipo de escucha pasiva, llevó a avances de cifrado importantes que generaron, en ocasiones, un exceso de confianza. Se creía que las complejas máquinas de cifrado de rotores de Alemania eran indescifrables, pero los errores de usuario y los esfuerzos a escala industrial de Gran Bretaña le permitieron descifrar los códigos alemanes. Con actualizaciones de bajo costo de sus equipos y claves, Alemania podría haber imposibilitado esa ventaja de Gran Bretaña, pero la confianza excesiva de Berlín en su cifrado impidió dichas alteraciones, lo que permitió la interceptación de información que cambió el curso de la guerra. El cifrado de extremo a extremo es mucho más avanzado que los intentos anteriores de cifrado, pero la historia sugiere que se debe ser humilde.

9. **Muchos estados desestiman los esfuerzos extraordinarios que puede realizar un adversario para violar la seguridad de sus redes.** Entre los debates sobre las telecomunicaciones modernas, vale la pena señalar que los estados que priorizaron la conveniencia o el comercio y que, por lo tanto, tomaron atajos de seguridad, a menudo se vieron sorprendidos negativamente por los esfuerzos de un adversario determinado para violar la seguridad de sus redes. En la Primera Guerra Mundial, Alemania se sorprendió por la velocidad y la implacabilidad con la que Gran Bretaña cortó todos los cables que Alemania utilizaba para acceder al mundo exterior; asimismo, los comandantes rusos se sorprendieron cuando su indisciplina radial condujo a la desastrosa derrota de Tannenberg. En la Segunda Guerra Mundial, Alemania no esperaba que los británicos construyeran una operación de descifrado de códigos altamente centralizada y de escala industrial que pudiera aprovechar los errores de comunicación alemanes, sin importar lo triviales o breves que fueran, para descifrar sus códigos. Y durante la Guerra Fría, los soviéticos nunca cifraron una línea telefónica submarina que creían que estaba fuera del alcance de Estados Unidos, sin embargo, Washington encontró la forma de interceptarla, lo que le permitió obtener una invaluable fuente de información.

10. **La seguridad de la red no solo se trata de interceptación, sino también de denegación.** Algunos de los debates sobre el papel de Huawei en las redes enfatizan las cuestiones de seguridad de los datos, pero desestiman el beneficio de dar mayor importancia a la

denegación de la red, que ha sido una parte importante de la competencia de las telecomunicaciones entre las grandes potencias. En los inicios de la telegrafía, las grandes potencias se propusieron cortar los cables y denegar las comunicaciones a sus adversarios, lo que culminó con la operación sin precedentes y bien planificada de Gran Bretaña de cortar todos los cables alrededor del mundo que pudieran conectar a Alemania con el exterior. En ocasiones, un estado puede perjudicarse a sí mismo con sus estrategias de denegación de redes, pero no dudará en aplicarlas si cree que el daño para su oponente será mayor.

Las grandes potencias y las telecomunicaciones

"Los grandes imperios se esforzaron enormemente para acelerar el flujo de la información", señala una historia de las telecomunicaciones. "Los romanos construyeron caminos, los persas y los mongoles establecieron postas de caballos, los británicos subsidiaron barcos de vapor de correo".[2] Pero, por mucho que los estados ansiaran información, los flujos de esta se mantuvieron limitados hasta los inicios del telégrafo moderno. La electrificación de los flujos de información creó las telecomunicaciones modernas y, junto con estas, los patrones conocidos de rivalidad de las grandes potencias por dichas telecomunicaciones.

Esas primeras décadas de las telecomunicaciones modernas, que abarcan desde 1840 hasta la Primera Guerra Mundial, comparten características importantes con el momento actual. Ese período, al igual que la actual época de la post-Guerra Fría, fue de relativa paz entre las grandes potencias, que hizo que los estados líderes fueran "menos sensibles" a cuestiones de política y seguridad en las redes de telecomunicaciones.[3] A medida que las grandes potencias extendían redes nacionales e internacionales en el siglo XIX, muchos se conformaban con dejar a cargo a la industria, desestimar la nacionalidad de las empresas privadas y quitarles importancia a los riesgos de que un adversario controlara las redes de telecomunicaciones. Los beneficios de los cambios revolucionarios en las telecomunicaciones (lo que algunas personas en el momento llamaban "la aniquilación del tiempo y del espacio")[4] eran tan obvios y abrumadores que la mera "propiedad de los cables se veía como un tema menor".[5] La telegrafía se relacionaba más con los negocios que con la política en ese período, según indica un historiador en una observación que bien se podría haber aplicado al entusiasmo inicial acerca de la tecnología de la información moderna y su encarnación más reciente: la 5G.[6]

El período de relativa complacencia de las grandes potencias no duraría. Estados como Perú en 1879 y, a continuación, Estados Unidos en 1898 fueron algunos de los primeros en cortar las redes de telecomunicaciones de un rival. A medida que las tensiones entre las grandes potencias aumentaban, los estados de todo el mundo se dieron cuenta de que algunos (a saber, Gran Bretaña) habían aprovechado bien el largo tiempo de paz y, a través de sus empresas privadas, habían obtenido un dominio de las comunicaciones internacionales.

Cada vez más preocupados por su dependencia de las redes de cables submarinos británicos, estados como Francia y Alemania subsidiaron fuertemente el desarrollo de sus propias redes, en un esfuerzo no muy distinto de los subsidios y la protección que aplica China a sus campeones de tecnología de la información, como Alibaba, Baidu, Tencent y Huawei. Y, tal como documenta la historiadora Heidi Tworek, los rivales de Gran Bretaña también hicieron apuestas importantes sobre la siguiente generación de tecnología de telecomunicaciones ("telegrafía sin hilos", mejor conocida como radio), con la esperanza de disminuir la dependencia de cables telegráficos submarinos de propiedad británica.[7] Mientras Gran Bretaña lideraba en este campo, Alemania se negó a confiar en las redes británicas. Construyó su propia red con campeones respaldados por el estado invirtiendo en áreas del mundo menos conectadas (Latinoamérica, África, Asia), en lo que se asemeja hoy en día a la expansión de las empresas tecnológicas chinas en el mundo en desarrollo y la determinación de Pekín de sentar las bases de las redes 5G.

Durante este período, los estados tomaban muy en serio muchos de los elementos de la competencia de las telecomunicaciones de las grandes potencias que, actualmente, a menudo se subestiman. Alemania, frustrada por el dominio británico en las redes radiales, utilizó un organismo normativo para ponerle fin a este, una táctica que demuestra que dichos organismos no eran menos importantes en esa época de lo que son actualmente. Y, a medida que las telecomunicaciones se volvieron inalámbricas y aún más fáciles de interceptar, las grandes potencias pusieron su confianza en el cifrado, a veces renunciando a la operación disciplinada de sus redes, en el supuesto de que las claves (pasos detallados para cifrar o descifrar mensajes) resolverían el problema, una creencia que casi siempre demostró ser errónea debido a los errores de usuario. Esa visión tiene un paralelo asombroso con los supuestos modernos sobre la inseguridad general de las redes de telecomunicaciones y la creencia, manifestada por algunas personas en los debates sobre Huawei, de que el cifrado neutralizaría significativamente el riesgo de que China accediera a redes de telecomunicaciones ajenas.

Cuando terminó la paz entre las grandes potencias y estalló la guerra, la importancia política de las telecomunicaciones (no siempre clara en tiempos de paz) se volvió evidente de manera repentina. El éxito alemán en la interceptación de las transmisiones rusas en la Primera Guerra Mundial produjo una victoria tan aplastante en la Batalla de Tannenberg que cambió el curso de la guerra y contribuyó a precipitar la salida de Rusia del conflicto. El dominio británico en cuanto a cables submarinos en la Primera Guerra Mundial fue, también, tan absoluto que aisló a Alemania del sistema de telecomunicaciones global, obligó a que los alemanes realizaran sus comunicaciones por cable a través de redes británicas y, finalmente, permitió descubrir el telegrama Zimmermann, que contribuyó a que Estados Unidos entrara en el conflicto. En la Segunda Guerra Mundial, Gran Bretaña obtuvo otro éxito de inteligencia descifrando el cifrado alemán, que se había creído indescifrable, lo que permitió conseguir una inigualable cantidad de información que, según la historia británica oficial, acortó en años la guerra en Europa. Estos casos demuestran que la seguridad en las telecomunicaciones no solo se trata de tácticas en el campo de batalla, sino de competencia política, que puede determinar los destinos de las grandes potencias y cambiar la historia del mundo.

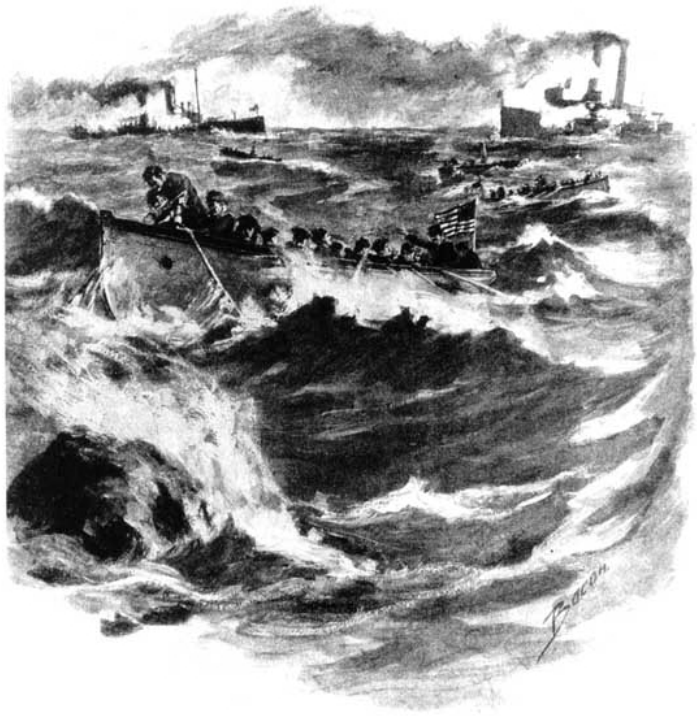
A medida que el mundo pasó a la Guerra Fría entre Estados Unidos y la Unión Soviética, las ventajas británicas quedaron desplazadas no solo por el poderío estadounidense, sino por cambios en la tecnología que volvieron a las redes más antiguas menos relevantes, lo que demuestra la importancia para las grandes potencias de mantenerse a la vanguardia de la tecnología. En esa nueva era, la competencia de las telecomunicaciones continuó en las líneas conocidas. Por ejemplo, Estados Unidos fue pionero en nuevas formas de interceptar cables submarinos que estaban enterrados tan profundamente y que se consideraban tan seguros que los mensajes a través de estos a menudo se dejaban sin cifrar. La competencia también se trasladó a otros dominios, como los satélites y la infraestructura de Internet, aunque gran parte de esta historia aún está en desarrollo y, en la mayoría de los casos, se mantiene secreta.

Las telecomunicaciones, como muestra esta breve serie de casos, siempre han sido políticas. La explotación de estas tecnologías y capacidades ha evolucionado generalmente junto con su desarrollo. Tan pronto como se creaban nuevos métodos de comunicación, las grandes potencias buscaban, generalmente, formas de interceptarlas o interrumpirlas. “Las comunicaciones eléctricas a menudo se han descrito como uno de los grandes logros de la humanidad”, señala un

historiador de las telecomunicaciones, “pero cuando lo vemos desde el punto de vista de la seguridad, vemos una imagen completamente diferente, dado que la seguridad no es una característica técnica, sino social y política”. Y "dado que la política no ha mejorado", señala, "las telecomunicaciones tienen un lado oscuro".[8]

Ahora, veamos un resumen de los temas clave en casi dos siglos de competencia de telecomunicaciones.

1. La guerra Hispano-Estadounidense: Los límites de la neutralidad de los cables



Representación de la expedición estadounidense de corte de cables en Cienfuegos, publicada en 1907. La operación demostró que los cables submarinos de telégrafos no se tratarían como neutrales durante los conflictos armados, incluso por parte de grandes potencias que, alguna vez, defendían la neutralidad de los cables.

Fuente: Naval Historical Center Online Library[9]

A medida que los cables submarinos comenzaron a surcar el mundo en el siglo XIX, varias potencias líderes, incluidas Francia, Alemania y Estados Unidos, pidieron mantenerlos al margen de la política internacional. En 1858, en uno de los primeros cables transatlánticos de la historia, el presidente de EE. UU., James Buchanan, instó a la reina Victoria a garantizar que las nuevas líneas telegráficas del mundo se mantuvieran "neutrales para siempre… incluso en medio de hostilidades".[10]

Sin embargo, una vez que estallaban las hostilidades, se abandonaban los principios moralistas de neutralidad. Dos décadas después del mensaje de Buchanan, Perú cortó las líneas de cables chilenas que pasaban por territorios en disputa.[11] Esa disputa recibió poca atención, pero cuando Estados Unidos, un antiguo campeón de la neutralidad de los cables, cortó cables en los océanos Atlántico y Pacífico durante la guerra Hispano-Estadounidense, el mundo lo notó.

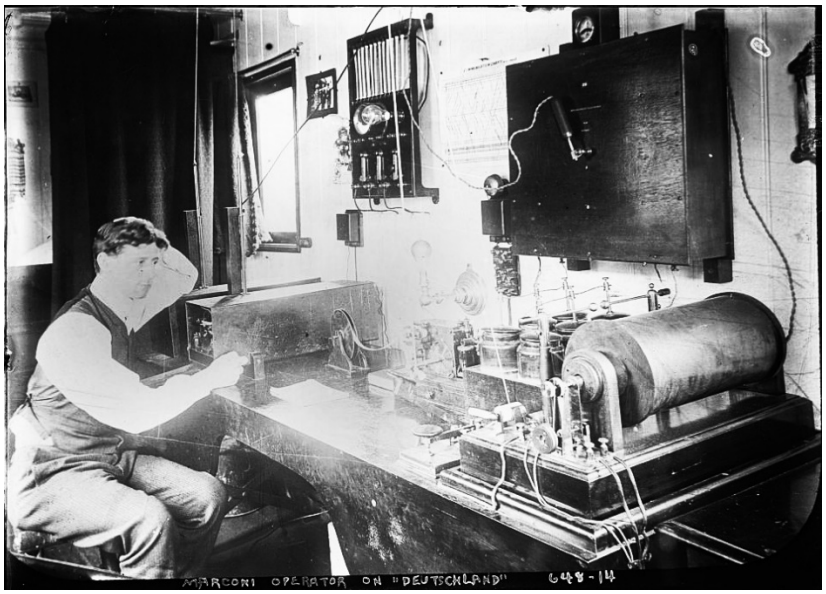
El corte de los cables por parte de Estados Unidos estaba planificado desde antes del conflicto. En el teatro del Atlántico, Estados Unidos esperaba cortar las comunicaciones entre España y sus fuerzas en Cuba. "El aislamiento de La Habana era, por supuesto, de vital importancia", indicó una revista estadounidense de la época, lo que requería que Estados Unidos "aislara a La Habana

de todas las comunicaciones telegráficas con el mundo exterior".[12] Estados Unidos comenzó cortando el tráfico español que atravesaba el territorio estadounidense en Florida. A continuación, envió un pequeño equipo estadounidense a destruir un nodo de telecomunicaciones clave en Cienfuegos, aislando a la ciudad de La Habana y gran parte del oeste de Cuba de España. Posteriormente, Estados Unidos atacó varios cables en el este de Cuba, así como en el Caribe, que conectaban Puerto Rico con España.[13] Juntos, el corte de los cables deterioró considerablemente la capacidad de España de dirigir y comandar fuerzas en Cuba.[14]

En el Pacífico, Estados Unidos cortó el único cable submarino entre Manila y Hong Kong, lo que efectivamente aisló a las Filipinas de España.[15] La decisión también dañó las comunicaciones de EE. UU., pero se supuso que infligiría un costo aún mayor para los españoles, y Estados Unidos podía compensarlo enviando un navío regularmente a Hong Kong para enviar despachos de vuelta a Washington.[16] Las fuerzas estadounidenses también cortaron los cables submarinos dentro de Filipinas, lo que deterioró aún más la capacidad de España de dirigir sus fuerzas.

La guerra Hispano-Estadounidense fue, quizás, el primer conflicto mundial que abarcó múltiples situaciones en que las telecomunicaciones eléctricas fueron importantes. También marcó la primera vez que una gran potencia procuró denegar el acceso a otro país a cables submarinos. Antes del conflicto, la telegrafía aún se veía como un ámbito principalmente comercial y muchas personas esperaban que los cables se mantuvieran al margen de competencias políticas y militares. El conflicto demostró los límites de tales perspectivas e indicó que el control de la infraestructura de las telecomunicaciones y la capacidad de denegar sus ventajas a los rivales geopolíticos siempre ha sido de importancia política fundamental.

2. La rivalidad angloalemana: Creación de redes y establecimiento de estándares



Operador de radio de la Compañía Marconi en la "sala Marconi" del trasatlántico alemán SS Deutschland. La influencia de la Compañía Marconi era tan grande que sus empleados operaban en salas de radio alemanas mientras Alemania se preocupaba de los riesgos de interceptación y denegación.

Fuente: Library of Congress, George Grantham Bain Collection[17]

El establecimiento de estándares tecnológicos y los efectos de red que este conlleva son una antigua y sutil escena de competencia entre las grandes potencias. Los estados cuyas tecnologías se convierten en el estándar dominante pueden ejercer poder sobre otros estados, algo de lo que están muy conscientes las potencias emergentes, que a menudo trabajan para reducir su vulnerabilidad creando sistemas paralelos. De hecho, la actual competencia entre China y Estados Unidos por la ICT se asemeja a la competencia de hace más de un siglo entre Alemania y Gran Bretaña por el dominio de la infraestructura de ICT de esa época, con asombrosos paralelos y lecciones clave para el presente.

A finales del siglo XIX, el ingeniero italiano Guglielmo Marconi, con el apoyo de la Marina Real Británica, creó la telegrafía sin hilos.[18] La invención fue revolucionaria. Mientras, en el pasado, las grandes potencias se habían cortado los cables entre sí, y las comunicaciones entre barcos y de los barcos a la costa habían sido difíciles, el sistema de Marconi resolvía esos problemas y era menos propenso a la interferencia.[19] Marconi terminó asociándose con Gran Bretaña, lo que le dio a ese país un monopolio sobre las transmisiones radiales. Cuando esto se combinó con el dominio del 60 % de la red de cables submarinos del mundo por parte de Gran Bretaña, dicho país dominó las transmisiones internacionales. La ventaja británica era inquietante para Alemania, pero la competencia sobre las tecnologías inalámbricas también “presentaba una oportunidad para que Alemania ejerciera el control sobre una nueva infraestructura internacional” y que “sorteara los cables británicos”; la primacía de las grandes potencias terminó en un empate.[20]

Al sentirse vulnerable, el káiser Guillermo II autorizó un apoyo directo del estado para los científicos e ingenieros alemanes, que lograron copiar los diseños de Marconi, los patentaron dentro de Alemania y crearon sus propias redes de radio financiadas por contratos con el ejército alemán.[21] Aun así, la ventaja de Marconi obtenida por la radio de largo alcance superior y por haber sido el pionero posicionó a su empresa con apoyo británico como el estándar global, y Marconi aprovechó estos efectos de red para fomentar una política de "no intercomunicación" con operadores de radio que no fueran Marconi. Las empresas y los trasatlánticos alemanes no deseaban quedar aislados de la comunicación global, por lo que prefirieron el sistema con apoyo británico a los sistemas alemanes.

El káiser Guillermo II intensificó la política industrial alemana para disputar el estándar británico. Rápidamente, decretó que dos grandes empresas de energía eléctrica alemanas que competían por desarrollos radiales, Siemens & Halske y AEG, se fusionaran para establecer la alternativa alemana definitiva: Telefunken. "La rivalidad [nacional] en el campo de la telegrafía sin hilos debilita la competitividad de Alemania", explicó el káiser, "y le da a la Compañía Marconi la oportunidad de alcanzar un monopolio mundial" que "no es para el bien de Alemania".[22] Bajo el mando del káiser Guillermo II, Alemania fomentó el proteccionismo prohibiendo los sistemas Marconi en algunos casos. Buscó mercados emergentes vendiendo su tecnología en Sudamérica y África para establecer el estándar en estas regiones y garantizar los ingresos.

Cuando esos esfuerzos demostraron ser insuficientes, Alemania logró el éxito en organismos normativos multilaterales. En 1906, Alemania reunió a las grandes potencias en la Primera Convención Radiotelegráfica Internacional, una conferencia sobre los estándares radiales. En esa ocasión, los miembros en conjunto prohibieron la política de "no intercomunicación" de Marconi, lo que rompió el monopolio británico y estableció un doupolio angloalemán de facto.[23]

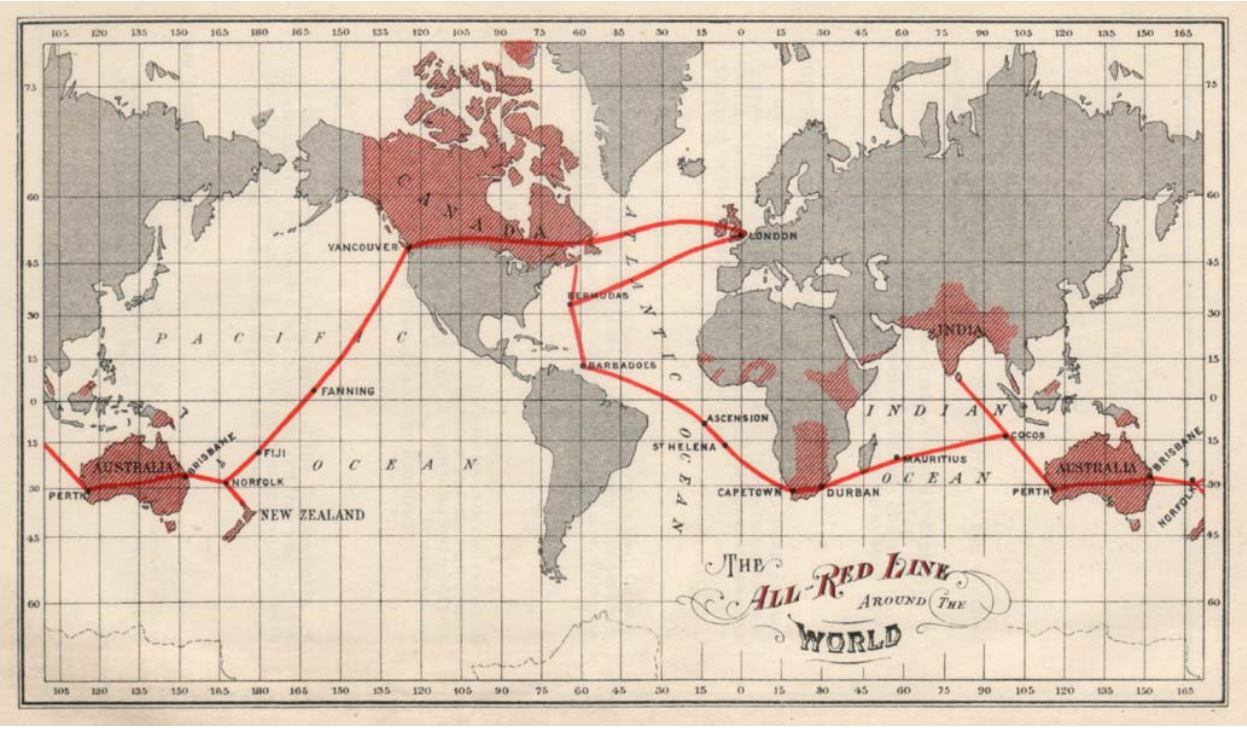
La competencia angloalemana revela que los organismos normativos poseen enormes implicaciones estratégicas. En la actualidad, China utiliza muchas de las técnicas que utilizaba Alemania hace un siglo: política industrial dirigida por el estado, protección estatal, generosos contratos estatales, integración cívico-militar, prohibiciones de productos rivales, fusiones forzadas, la búsqueda de mercados emergentes e, incluso, tratados internacionales para establecer sus estándares, todo lo cual ha ayudado a las empresas tecnológicas chinas, como Alibaba y Tencent, dueñas de WeChat y AliPay, a convertirse en campeones locales. Es así como estas empresas se han expandido en el extranjero, a menudo abordando no el mercado estadounidense, sino, al igual que la alemana Telefunken antes que ellas, mercados emergentes con menores utilidades y menor competencia.[24]

China también está disputando estándares en la infraestructura física de la conectividad de Internet. Su Gobierno está invirtiendo miles de millones para que los fabricantes de chips chinos venzan a los estadounidenses en la carrera por los estándares de Internet móvil 5G. Del mismo modo, empresas chinas como Huawei y ZTE reciben préstamos del Gobierno para fabricar la infraestructura física de conectividad de Internet en todo el mundo en desarrollo. Como lo demuestra el ejemplo británico, estos esfuerzos no solo convierten la tecnología China en el estándar, sino también ofrecen oportunidades de vigilancia. Mientras tanto, la Iniciativa de la Franja y la Ruta crea la posibilidad de que China establezca los estándares de "infraestructura

inteligente" en toda Asia, especialmente los sensores y el software pertinentes, y que les pueda negar a otras empresas la interoperabilidad, con lo que las excluiría de los vehículos autónomos y otras industrias.

La rivalidad angloalemana en la telegrafía demuestra que Washington debe tomar en serio el desafío dirigido por el Estado chino en cuanto a los estándares. También ofrece un camino a seguir. De la misma forma en que Alemania utilizó conferencias internacionales para romper el monopolio británico de la telegrafía, Estados Unidos podría establecer o preservar estándares de ICT favorables mediante acuerdos multilaterales. Esto puede impedir que China establezca estándares unilateralmente a través de sus acuerdos comerciales, campeones estatales o proyectos de infraestructura.

3. Gran Bretaña en la Primera Guerra Mundial: Despliegue de la hegemonía de la información



La "All Red Line", una costosa red de líneas de cables submarinos británicos construida con enormes redundancias y dispuesta de forma tal que ninguna parte pasara por territorios de un rival. La inversión insuficiente de Alemania en una red de telecomunicaciones global resiliente propia permitió a Gran Bretaña aislarla de las comunicaciones globales, mientras que Gran Bretaña, en general, no se vio afectada.

Fuente: George Johnson, ed., The All Red Line: The Annals and Aims of the Pacific Cable Project/Internet Archive[25]

Los esfuerzos de Alemania por romper el dominio británico de las telecomunicaciones a principios del siglo XX no nacieron de la paranoia. Cuando estalló la Primera Guerra Mundial, Gran Bretaña logró utilizar su considerable influencia en las redes de telecomunicaciones para dirigir el curso de la guerra. Cortó los cables alemanes, monitoreó las transmisiones alemanas y obligó a Alemania a comunicarse a través de redes controladas por Gran Bretaña, con lo que descubrió el telegrama Zimmermann, lo que contribuyó a que Estados Unidos entrara en la guerra.[26]

Gran Bretaña no fue la primera gran potencia que cortó o manipuló redes de telecomunicaciones: Perú había cortado una conexión entre Chile y Bolivia, Estados Unidos había cortado cables españoles y Gran Bretaña había aislado a los bóeres de sus partidarios europeos en una crisis y manipulado la comunicación por cables a Francia en otra.[27] Sin embargo, estos esfuerzos se llevaron al extremo durante la Primera Guerra Mundial.

Gran Bretaña fue la primera potencia en aislar a un país entero de las principales redes de telecomunicaciones globales, implementando, el primer día de la guerra, un plan diseñado

cuidadosamente en tiempos de paz.[28] En el período de un año, Gran Bretaña destruyó cables alemanes en todo el mundo: en el Canal de la Mancha, en el Mar del Norte, en el Atlántico Norte, en Sudamérica, en gran parte de África, en el Lejano Oriente e, incluso, en países neutrales que albergaban infraestructura alemana.[29]

Para compensar, Alemania intentó expandir la red de radio que Telefunken había construido una década antes en Latinoamérica y el "Sur Global" para que abarcara el mundo. En un esfuerzo con paralelos modernos en la Ruta de la Seda Digital de China, Berlín ofreció préstamos e inversiones a los gobiernos interesados en los “beneficios del desarrollo de la radio” con el fin de que albergaran nodos de comunicaciones alemanes. En respuesta, Gran Bretaña persuadió o indujo a la mayoría de estos países a renunciar al apoyo a los nodos de radio alemanes o los saboteó activamente.[30]

Sin redes propias, Berlín no tuvo más opción que depender de la red de Gran Bretaña durante la guerra. Al principio, los británicos comenzaron a monitorear silenciosamente todo el tráfico que pasaba por sus cables y utilizaron esta ventaja para librar una guerra de información contra Alemania, filtrando selectivamente tráfico alemán vergonzoso con el fin de dañar sus relaciones con los países neutrales. Cuando Alemania envió un telegrama para proponer una alianza militar con México en contra de Estados Unidos, el infame telegrama Zimmermann, dicho mensaje pasó por una red británica. Gran Bretaña lo interceptó, lo descifró y, a continuación, lo compartió con el Gobierno de Estados Unidos, que, a su vez, lo compartió con el público estadounidense.[31] Ese incidente contribuyó a que Estados Unidos entrara en la guerra, lo que cambió el curso de la historia del mundo y, finalmente, selló la derrota de Alemania.

La guerra de la información británica contra Alemania revela los peligros de proporcionar a una potencia rival la capacidad de monitorear el tráfico de otra o de interrumpir el acceso a las telecomunicaciones. Además, revela que las redes que las grandes potencias dan por sentadas en tiempos de paz, a menudo, no se pueden utilizar en tiempos de guerra, y que la guerra por los nodos de comunicación inevitablemente involucrará a terceros países o países neutrales.

4. Victoria alemana en Tannenberg: Los peligros de la interceptación

Una estación de telégrafo de campo inalámbrico alemana durante la Primera Guerra Mundial. La incapacidad de Rusia de cifrar suficientemente sus comunicaciones en sus estaciones de campo llevó a una derrota desastrosa que cambió el curso de la guerra.

Fuente: C. O. Nordensvan and Valdemar Langlet, Det stora världskriget *[The Great World War]*[32]

Alemania no carecía totalmente de capacidades propias en la guerra de la información. Cortó los cables sobre tierra y submarinos que conectaban a Rusia con sus aliados occidentales, así como varios cables transatlánticos de los que dependían los británicos, y fue pionera en el uso de submarinos para estas tareas.[33] Debido a la redundancia de las redes británicas, estos esfuerzos terminaron siendo menos debilitantes de lo que esperaban los alemanes. Lo que resultó ser mucho más eficaz fue el uso de inteligencia radial por parte de Alemania contra Rusia durante la Batalla de Tannenberg, en agosto de 1914, el primer mes de la guerra, lo que precipitó una derrota desastrosa para los rusos. Un oficial de inteligencia alemán de la época describió el incidente como "la primera vez en la historia de la humanidad en la que la interceptación del tráfico de radio enemigo jugó un papel decisivo".[34]

La batalla tuvo lugar en medio de victorias rusas en el frente oriental. Mientras Rusia penetraba más profundamente en Prusia Oriental, sus militares se encontraron con un considerable problema de comunicaciones, que creó las condiciones para una derrota desastrosa. Los alemanes en retirada habían cortado sus propias líneas telegráficas y los rusos que avanzaban carecían de suficiente personal capacitado para establecer comunicaciones por cable a través de su extensa formación. La transmisión por radio proporcionó una alternativa, pero, si bien los rusos habían adoptado nuevas tecnologías de radio para su comando y control militares, no las habían protegido suficientemente. Se habían asignado diferentes grupos a diferentes claves; la mayoría tenía poca capacitación en la codificación y la decodificación de señales; se sabía que los británicos habían descifrado algunos códigos; y los libros de códigos eran pocos o ininteligibles para muchos de los conscriptos analfabetos.[35] El resultado fue que los comandantes

rusos sintieron que tenían que correr el riesgo de utilizar mensajes de radio sin codificar y esperar que los alemanes no los estuvieran monitoreando cuidadosamente.

Sin embargo, los alemanes sí estaban monitoreando cuidadosamente las señales. Después de observar la indisciplina radial rusa en la guerra contra los japoneses, sabían que sus transmisiones no codificadas no formaban parte de una campaña de engaño. De esta forma, utilizaron su conocimiento de las comunicaciones rusas en tiempo real para levantar la "niebla de guerra" y derrotar decisivamente a una fuerza superior. Rusia perdió un ejército completo, con más de 100 000 bajas y 92 000 prisioneros, en comparación con solo 13 000 bajas alemanas.

5. Gran Bretaña en la Segunda Guerra Mundial: Los límites del cifrado

Rotores mecánicos de la máquina de cifrado Lorenz, considerados indescifrables durante la Segunda Guerra Mundial. Los esfuerzos británicos para descifrar la clave permitieron a los oficiales acceder a comunicaciones alemanas de alto nivel.

Fuente: Matt Crypto/Wikimedia Commons[36]

Las invenciones de la telegrafía sin hilos y la radio permitieron una mayor comodidad en relación con los cables físicos, pero implicaban un mayor riesgo de interceptación. En la Primera y la Segunda Guerras Mundiales, las grandes potencias existían en un mundo en el que se suponía que las comunicaciones radiales eran accesibles para terceros. Y en ese mundo, no muy diferente de los supuestos actuales sobre la vulnerabilidad de los sistemas computacionales y de telecomunicaciones modernos, el cifrado se consideraba fundamental para la seguridad. El resultado, como lo expresó un historiador militar estadounidense, fue una "lucha entre el criptógrafo y el analista de códigos".[37] Cuando las grandes potencias se encontraban en el lado incorrecto de esa lucha, los resultados podían ser catastróficos.

Para evitar este resultado, las organizaciones utilizaban claves para reducir el riesgo de que la interceptación arriesgara su seguridad. También aplicaban "disciplina radial" para evitar que los adversarios obtuvieran información sobre los patrones de uso a través del análisis del tráfico radial.

La mayoría de las grandes potencias se volcaron a un esfuerzo verdaderamente industrial para estudiar el tráfico del adversario y, de ser posible, descifrar sus claves. Gran Bretaña fue mucho

más centralizada en su análisis de las claves de sus adversarios que Alemania, que tenía esas funciones repartidas entre varios organismos. Y, al igual que el éxito británico en la inteligencia de señales y el análisis de códigos había cambiado el curso de la Primera Guerra Mundial, también lo hizo en la Segunda Guerra Mundial, cuando la operación británica en Bletchley Park descifró las claves alemanas Enigma y Lorenz.

Los sistemas de cifrado Enigma y Lorenz utilizaban máquinas de rotores extraordinariamente complejas para cifrar mensajes que Alemania creía que "se mantendrían invulnerables".[38] Cada vez que se presionaba una tecla, se reemplazaba un carácter por otro carácter según ajustes únicos para la máquina, y era necesario que tanto el emisor como el destinatario compartieran dichos ajustes (que, en el caso del sistema Lorenz, superaban el número total de átomos del universo) con el fin de leer el mensaje.[39] Las fuerzas armadas, la Gestapo y los diplomáticos utilizaban Enigma; Adolf Hitler y los oficiales militares y nazis superiores utilizaban Lorenz, que era aún más complejo, para comunicarse entre sí.

El éxito británico en descifrar Enigma y Lorenz fue producto de varios desarrollos. En primer lugar, fue producto de la cooperación de la inteligencia aliada con Polonia, que había aprovechado algunos errores alemanes para descifrar algunas máquinas Enigma más simples.[40] Según afirmó un analista de códigos británico de la época, su esfuerzo "ni siquiera hubiera podido empezar" sin las contribuciones polacas.[41]

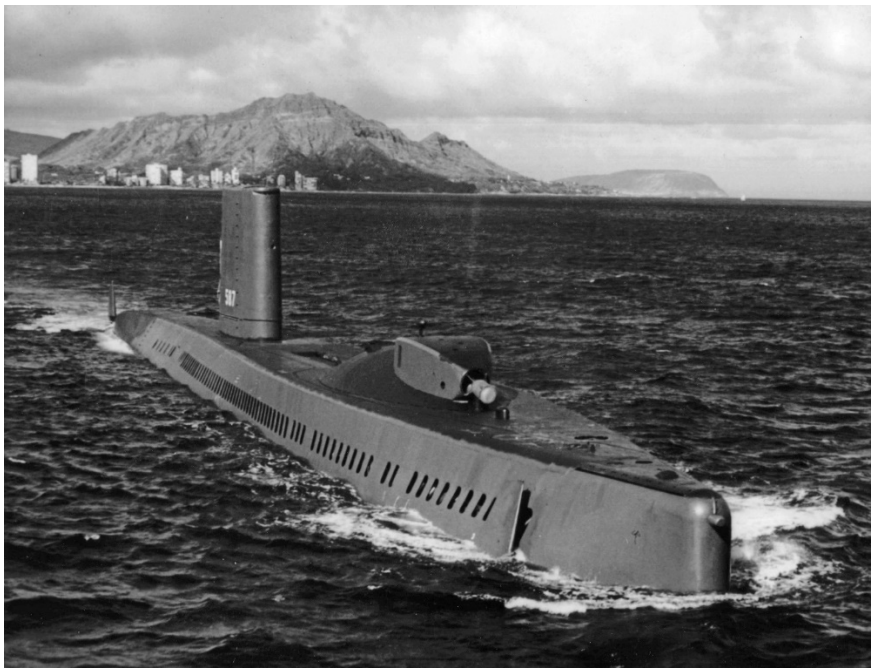
En segundo lugar, fue producto de la confianza excesiva de Alemania, que nunca sospechó que las claves se habían descifrado y, por lo tanto, renunció a realizar modificaciones bastante simples que hubieran obligado a Gran Bretaña a comenzar todo de nuevo.[42] Aun así, la fe alemana en la invulnerabilidad de sus máquinas "casi estaba en lo cierto", según narró un oficial superior de Bletchley Park.[43]

Por último, fue producto de un lapso único, pero importante, en la "disciplina radial" alemana, que creó una apertura para realizar ingeniería inversa de los sistemas de cifrado alemanes, a pesar de nunca haber visto uno realmente.[44] Incluso los sistemas más sofisticados eran vulnerables a errores de usuario y un adversario vigilante podría aprovecharlos.

El descifrado de Enigma y Lorenz le permitió a Gran Bretaña acceder a algunas de las comunicaciones más secretas de Alemania. Se dice que Winston Churchill consideró que la inteligencia fue un factor clave que permitió a Gran Bretaña ganar la guerra y que Dwight D. Eisenhower la llamó "decisiva".[45] El historiador oficial de inteligencia británica, Sir Francis Harry Hinsely, afirma que estos éxitos "acortaron la guerra, al menos, dos años, y probablemente cuatro", debilitando al mariscal de campo Erwin Rommel en África, revirtiendo las pérdidas de las naves aliadas por los submarinos alemanes y permitiendo los desembarcos en Normandía.[46] También permitieron a gran Bretaña identificar a prácticamente todos los espías alemanes que ingresaban al país y, a menudo, hacerlos cambiar de bando o utilizarlos para transmitir información falsa, ante lo que el jefe del programa observó que la inteligencia británica "dirigía y controlaba activamente el espionaje alemán en este país".[47] Pocos países han tenido un conocimiento tan íntimo de otro durante la guerra.

En su conjunto, los éxitos de Gran Bretaña contra Alemania, el monitoreo por parte de Polonia de las comunicaciones alemanas en tiempo de paz y su decisión de compartir sus descubrimientos con Gran Bretaña tienen lecciones aplicables al día de hoy, cuando las grandes potencias realizan reconocimiento cibernético contra otras. En términos más generales, las personas que sugieren que el cifrado mitiga los problemas de que un adversario obtenga acceso a la red de telecomunicaciones propia pueden estar cometiendo un error no muy distinto del que cometió Alemania alguna vez: exceso de confianza en la tecnología y poca atención a la siempre presente posibilidad del error humano.

6. Operación Ivy Bells: Las profundidades de la búsqueda de información



El USS Halibut, que se dice que estuvo involucrado en un esfuerzo de interceptación de una línea telefónica submarina soviética.

Fuente: U.S. Navy/Wikimedia Commons[48]

La Unión Soviética era mucho más cuidadosa con su cifrado de lo que habían sido los nazis, confiando en su propia versión de Enigma, conocida como Fialka, que era mucho más compleja.[49] Por ese motivo, la abundante información de nivel estratégico producida en la Segunda Guerra Mundial, después de descifradas las claves alemanas, no tuvo un análogo conocido públicamente en la Guerra Fría. Debido a estos desafíos, se probaron por primera vez otros métodos para penetrar las telecomunicaciones del adversario. Uno de los más audaces de estos esfuerzos se llevó a cabo con respecto a los cables submarinos.

Los inicios de los cables submarinos en el siglo XIX llevaron a esfuerzos para cortarlos y, ocasionalmente, interceptarlos, a menudo en aguas poco profundas o en tierra, donde estas tareas eran más fáciles de realizar. Por el contrario, la realización de estas operaciones en aguas profundas controladas por un adversario se consideraba prácticamente imposible, especialmente si se debían realizar de manera encubierta. A partir del siglo XX, los británicos y otras grandes potencias después de ellos habían llegado a una determinación acerca de la seguridad de los cables submarinos: si los lugares a donde los cables llegaban a tierra estaban protegidos y los cables no pasaban por países neutrales u hostiles, generalmente estarían protegidos de la interceptación y, a menudo, no correrían peligro de que los cortaran, especialmente en tiempos de paz.[50]

Mas durante la Guerra Fría, ese cálculo cambió. La llegada de los submarinos nucleares abrió la posibilidad de interceptar cables submarinos en aguas más profundas. Sin embargo, se pensaba que la tarea de enviar buzos para acceder a cables en la profundidad del lecho marino era más parecida a la exploración espacial que a los esfuerzos conocidos en cuanto a la manipulación de cables intentados en épocas anteriores. La creación de una interceptación que se pudiera instalar en esas condiciones también era técnicamente difícil.

Cuando Estados Unidos sospechó que un cable submarino soviético podría extenderse desde el cuartel general de la marina en Vladivostok hasta una base de submarinos en la península de Kamchatka, buscó superar estos obstáculos, lo que demostró el valor de la inteligencia de las señales.[51] Se pensaba que la interceptación de ese hato de cables de cinco pulgadas proporcionaría información fundamental sobre las fuerzas nucleares soviéticas.[52] Si bien los soviéticos cifraban todo el tráfico enviado por el aire, Estados Unidos esperaba que los soviéticos supusieran que era prácticamente imposible acceder al tráfico a través del cable submarino protegido y que, por lo tanto, no lo cifrarían. Además, "los almirantes y generales soviéticos serían demasiado imperiosos e impacientes para soportar a un ejército de criptógrafos ya abrumados por la sola carga de su trabajo" e insistirían en realizar comunicaciones de voz no protegidas.[53] De esta forma, una interceptación proporcionaría un tesoro poco común de información, y la marina estadounidense lanzó la operación Ivy Bells para establecerlo.

Mucho acerca de la interceptación y la información recopilada gracias a esta se mantiene clasificado, pero los recursos abiertos ofrecen algunos detalles sobre esta operación única e innovadora. Estados Unidos envió un submarino nuclear, el USS Halibut, para burlar sigilosamente a la marina soviética y buscar el cable submarino en una zona de 600 000 millas cuadradas.[54] Se creó tecnología innovadora para garantizar que los buzos pudieran trabajar bajo grandes presiones y en temperaturas extremadamente frías durante varias horas. Del mismo modo, se idearon nuevos métodos para instalar interceptaciones en este difícil entorno.[55] Todo esto debía realizarse sin que los soviéticos lo detectaran ni sospecharan. Si se detectaba la nave, los soviéticos podrían abordarla o destruirla.

Por último, la operación fue exitosa y, durante toda la década de 1970, la marina estadounidense interceptó y grabó mensajes no protegidos que se transmitían a través del cable. Con una frecuencia de algunos meses, los submarinos estadounidenses entraban sigilosamente en aguas soviéticas, evadían submarinos de ataque, desplegaban buzos en las líneas de cable interceptadas y extraían cintas de las comunicaciones soviéticas, lo que constituía un tesoro de información extremadamente valioso y poco común. Si bien Estados Unidos había extendido una "red de satélites, aviones, estaciones de escucha y submarinos espía" para recopilar información de señales, "no podía penetrar en una línea telefónica física" en el territorio de un adversario. Este esfuerzo ilustró el cambio evolutivo en las telecomunicaciones, a saber, que un determinado actor con las herramientas adecuadas podía acceder a datos y señales transmitidos a través de cualquier medio. Si bien esta interceptación finalmente se reveló producto de una filtración, proporcionó invaluable información militar y política a Estados Unidos y a sus aliados.[56]

La competencia de las telecomunicaciones modernas en una perspectiva histórica

Hacia el final de la Guerra fría, Estados Unidos había reemplazado claramente a Gran Bretaña como la superpotencia de la información. Estados Unidos mantuvo una posición nodal en la Internet global, sólidas capacidades espaciales, dominio en la mayoría de las tecnologías de Internet y, según algunas revelaciones públicas, capacidades sofisticadas de interceptar comunicaciones de sus adversarios o, posiblemente, denegarlas.

Actualmente, estas ventajas estadounidenses se están poniendo a prueba, al igual que las de Gran Bretaña hace más de un siglo. Hoy en día Rusia y, especialmente, China desafían el dominio de EE. UU. Si bien Estados Unidos goza de una posición nodal en muchos flujos de datos, otras potencias buscan cada vez más reducir su dependencia de las redes estadounidenses. Al mismo tiempo, la posición nodal estadounidense es menos necesaria para la interceptación de lo que fue la de Gran Bretaña hace un siglo. Internet posibilita las intrusiones sin necesidad de tener el control sobre la infraestructura física. Los teléfonos inteligentes y las redes informáticas se pueden jaquear, y los resultados de que las comunicaciones secretas de un país se pongan en peligro producto de estas intrusiones virtuales son los mismos que los de las interceptaciones físicas de épocas anteriores. La conexión de esta manera probablemente crea una mayor vulnerabilidad ahora que en la era del telégrafo o de la radio inalámbrica.

Rusia ha sido un estado líder en la explotación de esa vulnerabilidad. En el 2007, Rusia lanzó una serie de ataques cibernéticos contra las instituciones de Estonia, principalmente ataques distribuidos de denegación de servicio.[57] En el 2008, inició ataques cibernéticos en la guerra ruso-georgiana. Estos ataques no solo incluyeron ataques dirigidos de denegación de servicio, sino también esfuerzos para redirigir los sitios web del Gobierno, apoderarse de servidores gubernamentales georgianos y redirigir el tráfico de Internet de Georgia a través de servidores controlados por Rusia, algunos de los cuales se organizaron con anterioridad al conflicto, de manera que coincidieran con la acción militar rusa.[58] En el 2014, cuando Rusia invadió Crimea, se combinaron ciberataques con el control físico de las redes de telecomunicaciones. Los soldados rusos tomaron el control de instalaciones de telecomunicaciones ucranianas, las que utilizaron para interrumpir la comunicación en Crimea e, incluso, para llevar a cabo ciberataques e interrupciones en otras partes de Ucrania.[59] En el 2015, Rusia comenzó una serie de ciberataques a la infraestructura ucraniana que dejaron sin electricidad a cientos de miles de ucranianos en dos ocasiones principales. Durante los siguientes años, procedió a lanzar una ola de ataques sin precedentes en toda Ucrania, que abarcaron "medios de comunicación, finanzas, transporte, las fuerzas armadas, la política y la energía" (prácticamente todos los segmentos de la sociedad ucraniana), en lo que algunas personas creen que fue, parcialmente, un esfuerzo de entrenamiento para una campaña similar contra Estados Unidos.[60] Al mismo tiempo, continuó con una variedad de ataques en todos los estados bálticos y, como es sabido, intentó interferir en las elecciones de EE. UU. en el 2016 y en el 2020 con campañas de desinformación, así como en otros países.[61] En el 2021, el Gobierno de EE. UU. acusó formalmente a Rusia del jaqueo de la empresa de TI SolarWinds, un ataque sofisticado que puso en riesgo gran parte del Gobierno federal y varias empresas importantes de EE. UU.[62]

China es otra gran potencia que realiza importantes inversiones en la competencia de las telecomunicaciones, aunque, a diferencia de Rusia, los esfuerzos de China no solo buscan aprovechar la infraestructura de Internet existente, sino también crear redes e infraestructura en la que pueda influir o que pueda, incluso, controlar. Al igual que Rusia, China ha sido hábil para explotar las vulnerabilidades de Internet existentes. A principios de la década del 2000, inició una ola de ataques a las redes del Departamento de Defensa de Estados Unidos, lo que el Departamento denominó Operación Titan Rain.[63] Gobiernos de todo el mundo (Estados Unidos, Reino Unido, Francia, Alemania, Canadá, Australia, Japón, Corea del Sur, Taiwán, la India y muchos otros) se han quejado de la intrusión China en sus redes gubernamentales. El fiscal general de Estados Unidos, William Barr, confirmó que algunos de los ataques cibernéticos más grandes de la última década fueron obra de agentes chinos, lo que incluyó robos de registros de la Oficina de Gestión de Personal de Estados Unidos (registros de 21 millones de personas), de hoteles Marriott (de 400 millones), de seguros de salud Anthem (de 80 millones) y de Equifax (de 147 millones), entre otros.[64]

Al mismo tiempo, China también está sentando las bases para una futura infraestructura de Internet y, a la luz de sus esfuerzos anteriores, es poco probable que dichos esfuerzos sean estrictamente comerciales ahora o que lo sigan siendo en el futuro. Las inversiones de China son mayores en las redes 5G, que se espera que formen la base de una economía más inteligente y conectada, que conecte un sinnúmero de dispositivos y sensores. Ansiosa por crear estas redes en todo el mundo, China ha subsidiado sus campeones y proyectos de 5G en todo el mundo como parte de una iniciativa de Ruta de la Seda Digital. Gracias a sus precios competitivos, empresas como Huawei pudieron superar a otros proveedores importantes de 5G y dominar una participación considerable en el mercado global, que convierte a China en un líder en la construcción de estas redes. Y, aparte de la red 5G, el Gobierno de China ha subvencionado esfuerzos para construir infraestructura de Internet o de comunicaciones en prácticamente todos los continentes. Todos estos esfuerzos van acompañados de una campaña para establecer los estándares globales, una prioridad de la política clave para China, consagrada en documentos de planificación de alto nivel que, al igual que la rivalidad angloalemana por la radio hace un siglo, podría forjar el futuro de las telecomunicaciones en formas ventajosas para China. Para ese fin, China recientemente reveló una nueva iniciativa de seguridad de datos.[65]

Algunas personas temen que las actividades de China abran la puerta a la posibilidad de que Pekín tenga el control de facto de estas redes, ya sea para interceptar tráfico o denegar el acceso. Se dispone de poca información pública sobre los esfuerzos de China para adquirir dicho control, pero el Gobierno de EE. UU. reveló en febrero del 2020 que Huawei tenía puertas traseras en sus equipos de red, que no las reveló a las empresas pertinentes con las que suscribió contratos y que dichas puertas traseras iban más allá de lo que los gobiernos anfitriones a veces solicitan como parte de interceptaciones lícitas.[66] Además, los informes públicos revelaron que Huawei ha ayudado a gobiernos, como al de Uganda y Zambia, facilitándoles las identidades de ciertos disidentes.[67] Incluso aparte del caso de Huawei, una empresa de ciberseguridad descubrió recientemente puertas traseras en software tributario obligatorio que el Gobierno chino exige que las empresas extranjeras instalen.[68] Independientemente de si estos casos indican que Huawei ha aprovechado su posición en estas redes, el comportamiento de la empresa y el historial de China respecto de los ciberataques y el espionaje son motivos de preocupación.

El otro motivo importante de preocupación proviene de la historia y del comportamiento de, incluso, grandes potencias liberales, limitadas más estrictamente por el imperio de la ley. De hecho, los casos históricos anteriores indican claramente que el Gobierno chino probablemente aprovechará el tipo de poder e influencia del que goza una empresa como Huawei, de la misma forma que otras grandes potencias han aprovechado la posición de sus empresas o capacidades en telecomunicaciones.

Desde esa perspectiva histórica más amplia, la evidencia puede llevar a muchos observadores a concluir que se necesita prudencia sobre el papel de Huawei en las redes de telecomunicaciones, aunque los motivos de la empresa sean estrictamente comerciales, sus promesas de "sin puerta trasera y sin espionaje" sean creíbles y Pekín sea sincero en su intención de respetar dicho compromiso.

En términos más generales, según muestra este informe, muchas de las características de la competencia de las telecomunicaciones entre las grandes potencias que se consideran nuevas hoy en día tienen sus raíces en el pasado. En la historia, los siguientes elementos se han repetido varias veces:

- *Poder:* El control sobre las redes de telecomunicaciones ha sido una forma de poder político desde su creación hace más de 150 años. Gran Bretaña aprovechó su papel en las telecomunicaciones y la radio, es probable que Estados Unidos lo haya hecho en la era moderna de Internet y existen motivos para preocuparse de que China pueda intentar hacerlo hoy.

- *Complacencia*: Los largos períodos de paz y prosperidad han conducido a la complacencia sobre los riesgos de las telecomunicaciones. En el siglo XIX, las grandes potencias se conformaban con depender de empresas extranjeras y redes operadas por extranjeros, de la misma forma en que los estados hoy han estado dispuestos a aceptar los equipos y la operación de telecomunicaciones chinas. Sin embargo, con el tiempo, la dependencia de posibles competidores y adversarios demostró ser desastrosa para países como Alemania y redefinió la política mundial.

- *Explotación:* La nueva tecnología de telecomunicaciones ha llevado siempre a nuevos esfuerzos por interceptarla, denegarla o explotarla. A pesar de la esperanza de que el cifrado pueda complicar los esfuerzos de China de interceptar las comunicaciones modernas, la gran confianza que se tuvo en el cifrado en períodos pasados terminó hecha añicos debido a los errores de usuario y a los esfuerzos determinados de estados rivales por descifrarlo, como descubrió Alemania cuando Gran Bretaña descifró sus claves supuestamente "indescifrables". Cada ola de tecnologías supuestamente seguras se debe acompañar de humildad.

- *Campeones:* Los estados a menudo buscan sus propios campeones de telecomunicaciones, especialmente a medida que aumentan las tensiones entre las grandes potencias. El Gobierno de China se enorgullece de los logros de Huawei y la defiende en todo el mundo, incluso amenazando a los estados que se niegan a utilizar su tecnología. Sería inusual que una empresa tan cercana a su Gobierno local fuera inmune a

la presión estatal cuando tantos otros campeones de telecomunicaciones en la historia no lo han sido.

- *Estándares*: Los estándares de telecomunicaciones pueden determinar quién ejerce poder de red, como lo ejemplifica el caso de Alemania, que utilizó un organismo normativo para romper el dominio de Gran Bretaña en la radio inalámbrica. Hoy en día, esa competencia se desarrolla en organismos como la Unión Internacional de Telecomunicaciones y el papel de Huawei en esta indica la necesidad de considerar si sus estándares permitirán que China dé nueva forma a las telecomunicaciones.

- *Denegación:* La seguridad de la red no solo se trata de interceptación y seguridad de los datos, sino también de denegación de toda la operación de la red o del acceso a redes externas. Gran Bretaña aisló a Alemania de las redes telegráficas mundiales, de la misma forma en que el papel de Huawei en sus redes podría permitirle desactivar redes en países en los que opera equipos aunque no pueda acceder fácilmente a los datos.

- *Determinación:* Muchos estados subestiman los esfuerzos extraordinarios que puede realizar un adversario para violar la seguridad de sus redes y se llevan una sorpresa desagradable cuando lo hace. La capacidad de Gran Bretaña de descifrar las claves alemanas en la Segunda Guerra Mundial a través de esfuerzos de escala industrial y la capacidad estadounidense de interceptar cables submarinos soviéticos internos supuestamente inviolables demuestra los extremos a los que las grandes potencias están dispuestas a llegar para acceder a información de señales crítica. Es probable que China también realice estos esfuerzos extraordinarios, y aunque a Huawei le sea difícil utilizar como arma su posición en las redes modernas, subestimar la inventiva y el empuje de un competidor determinado como China es un tema recurrente en la competencia de las telecomunicaciones.

Como lo demuestra este informe, muchas de las características del juego de las grandes potencias por las telecomunicaciones se mantienen iguales, aunque los jugadores sean diferentes.

Acerca de los autores

Rush Doshi fue director de Iniciativa Estratégica de China de Brookings y miembro de la Política Exterior de Brookings. También fue miembro del Centro Chino Paul Tsai de la Escuela de Derecho de Yale y fue parte de la clase inaugural de Wilson China. Su investigación se centró en la gran estrategia de China y en los problemas de seguridad del Indo-Pacífico. Doshi es el autor de *The Long Game: China's Grand Strategy to Displace American Order [El juego extenso: la gran estrategia de China para reemplazar el orden estadounidense]*, que será publicado próximamente por Oxford University Press. Actualmente trabaja en la administración de Biden.

Kevin McGuiness trabajó recientemente con Brookings como participante externo del Programa Skillbridge del Departamento de Defensa, en que contribuyó en varios proyectos en el Centro para Estudios de Política de Asia Oriental. Es un veterano de la Fuerza Aérea y recientemente terminó su período de servicio como docente de la Academia de la Fuerza Aérea de los Estados Unidos, a cargo de cursos en relaciones internacionales y política asiática. Recientemente, trabajó como asistente de investigación del Centro de Estudios de Asuntos Militares Chinos del Instituto de Estudios Estratégicos Nacionales, en donde se concentró en los temas de la modernización del Ejército Popular de Liberación y la seguridad en el Indo-Pacífico.

Reconocimientos

Los autores desean agradecer a los expasantes Isabella Lu, Zijin Zhou y Gaoqi Zhang por su colaboración en la investigación para este proyecto, a varios revisores anónimos, a Claire Harrison y Ted Reinert por editar el informe y a Chris Krupinski y Rachel Slattery por el diseño web. Brookings agradece al Departamento de Estado de EE. UU. y al Instituto de Informes de Paz y Guerra por financiar esta investigación.

Este informe se completó antes del servicio gubernamental de Rush Doshi, incluye solo fuentes abiertas y no refleja necesariamente la política o posición oficial de ningún organismo del Gobierno de los EE. UU.

[1] Steven Chase, Robert Fife, and Barrie McKenna, "Trudeau Refuses to Let 'politics Slip into' Decision on Huawei," The Globe and Mail, October 15, 2018, https://www.theglobeandmail.com/politics/article-trudeau-refuses-to-let-politics-slip-into-decision-on-huawei/; Greg Quinn and Josh Wingrove, "Trudeau Says Politics Won't Factor Into Huawei 5G Decision," Time, 19 de diciembre del 2018, https://time.com/5485141/justin-trudeau-huawei-5g-decision-politics/.

[2] Daniel R. Headrick, The Invisible Weapon: Telecommunications and International Politics, 1851-1945 (Oxford, U.K.: Oxford University Press, 1991), capítulo 1.
[3] Ibíd., esta observación es de Headrick.
[4] Ibíd.
[5] Ibíd.
[6] Ibíd., esta observación es de Headrick.
[7] Heidi Tworek, News from Germany: The Competition to Control World Communications, 1900-1945 (New York: Harvard Historical Studies, 2019).
[8] Daniel R. Headrick, The Invisible Weapon.
[9] "NH 79949 Cienfuegos Cable-Cutting Operation, 11 May 1898," Naval Historical Center Online Library, https://www.history.navy.mil/content/history/nhhc/our-collections/photography/us-people/b/baker-benjamin-f/nh-79949.html.
[10] Ibíd., capítulo 5.
[11] Jonathan Winkler, "Information Warfare in World War I," The Journal of Military History 73, No. 3 (2009): 845–67, https://doi.org/10.1353/jmh.0.0324.
[12] Cameron McR. Winslow, "Cable-Cutting at Cienfuegos," The Century Illustrated Monthly Magazine 57 (1899): 708-717, https://books.google.com/books?id=Y7fPAAAAMAAJ&pg=PA708#v=onepage&q&f=false.
[13] Jonathan Winkler, "Silencing the Enemy: Cable-Cutting in the Spanish–American War," War on the Rocks, 6 de noviembre del 2015, https://warontherocks.com/2015/11/silencing-the-enemy-cable-cutting-in-the-spanish-american-war/; Rebecca Raines, "Manifesting Its Destiny: The U.S. Army Signal Corps in the Spanish-American War," *Army History* 46 (1998): 14–21, https://www.jstor.org/stable/26304991.
[14] Jonathan Winkler, "Silencing the Enemy."
[15] "Spanish American War: Telegraphy and Cable Cutting, Introductory Essay," Naval History and Heritage Command, https://www.history.navy.mil/research/publications/documentary-histories/united-states-navy-s/telegraphy-and-cable.html.
[16] Jonathan Winkler, "Silencing the Enemy."
[17] Library of Congress, George Grantham Bain Collection, https://www.loc.gov/pictures/item/2014683102/.
[18] Aunque, según señala Heidi Tworek, su propia función se ha inflado en el desarrollo de esta tecnología. Heidi Tworek, *News from Germany*.
[19] Marc Raboy, "The First Company That Wanted to 'Connect the World' Wasn't Google or Facebook," Media@LSE, 24 de agosto del 2016, https://blogs.lse.ac.uk/medialse/2016/08/24/the-first-company-that-wanted-to-connect-the-world-wasnt-google-or-facebook/.
[20] Heidi Tworek, News from Germany, 12–13.
[21] Michael Friedewald, "Telefunken vs. Marconi, or the Race for Wireless Telegraphy at Sea, 1896-1914," SSRN (9 de enero del 2014): https://doi.org/10.2139/ssrn.2375755.
[22] Ibíd.
[23] Marc Raboy, Marconi: The Man Who Networked the World (Oxford, U.K.: Oxford University Press, 2016), 226–28.
[24] Por ejemplo, Telefunken tenía actividades incluso en áreas en que Alemana no tenía una presencia colonial importante, como Latinoamérica.
[25] George Johnson, ed., *The All Red Line: The Annals and Aims of the Pacific Cable Project* (Ottawa: James Hope and Sons, 1903), 10, en Internet Archive, https://archive.org/details/allredlineannals00johnuoft/page/n11/mode/2up.
[26] Gordon Corera, "How Britain Pioneered Cable-Cutting in World War One," BBC News, 15 de diciembre del 2017, https://www.bbc.com/news/world-europe-42367551.
[27] Jonathan Winkler, "Information Warfare in World War I," 847.
[28] P. M. Kennedy, "Imperial Cable Communications and Strategy, 1870-1914," The English Historical Review 86, No. 341 (1971): 728–52, https://www.jstor.org/stable/563928.
[29] Jonathan Winkler, "Information Warfare in World War I," 849.
[30] Ibíd., 851.
[31] Gordon Corera, "Why Was the Zimmermann Telegram so Important?," BBC News, 17 de enero del 2017, https://www.bbc.com/news/uk-38581861; Patrick Beesly, Room 40: British Naval Intelligence 1914-18 (San Diego: Harcourt Brace Jovanovich, 1982).
[32] C. O. Nordensvan and Valdemar Langlet, *Det stora världskriget* [The Great World War] (1915), en Wikimedia Commons, https://commons.wikimedia.org/wiki/File:German_WW_I_field_telegraph_002.jpg.
[33] Jonathan Winkler, "Information Warfare in World War I."

[34] Wilhelm Flicke, "The Beginnings of Radio Intercept in World War I: A Brief History by a German Intelligence Officer," NSA Cryptologic Spectrum Articles 8, No. 2 (1978): 21, https://www.nsa.gov/news-features/declassified-documents/cryptologic-spectrum/.
[35] Bruce Norman, Secret Warfare: The Battle of Codes and Ciphers (Newton Abbot, U.K.: David & Charles Ltd, 1973); Prit Buttar, Collision of Empires: The War on the Eastern Front in 1914 (Oxford, U.K.: Osprey Publishing, 2014).
[36] Matt Crypto, "The rotors of a Lorenz SZ42 cipher machine on display at Bletchley Park museum," en Wikimedia Commons, https://commons.wikimedia.org/wiki/File:SZ42-6-wheels.jpg.
[37] George I. Beck, "Military Communication - The Advent of Electrical Signaling," Britannica, https://www.britannica.com/technology/military-communication.
[38] Harry Hinsley, "The Influence of ULTRA in the Second World War" (conferencia realizada en Cambridge, Reino Unido el 19 de octubre de 1993), http://www.cdpa.co.uk/UoP/HoC/Lectures/HoC_08e.PDF.
[39] $1x10^{170}$ ajustes posibles.
[40] "Bletchley Park Remembers Polish Code Breakers," BBC News, 14 de julio del 2011, https://www.bbc.com/news/uk-england-beds-bucks-herts-14141406.
[41] Gordon Welchman, The Hut Six Story: Breaking the Enigma Codes (Cleobury Mortimer, U.K.: Classic Crypto Books, 1997).
[42] Harry Hinsley, "The Influence of ULTRA."
[43] Ibíd.
[44] Consulte, por ejemplo, Jerry Roberts, Lorenz: Breaking Hitler's Top Secret Code at Bletchley Park (Cheltenham, U.K.: History Press, 2017).
[45] F. W. Winterbotham, The Ultra Secret (New York: Harper & Row, 1974), 154, 191.
[46] Harry Hinsley, "The Influence of ULTRA."
[47] Calder Walton, "The Spies Who Came In From the Continent," Foreign Policy, 27 de abril del 2019, https://foreignpolicy.com/2019/04/27/the-spies-who-came-in-from-the-continent-espionage-britain-brexit/.
[48] U.S. Navy, en Wikimedia Commons, https://commons.wikimedia.org/wiki/File:USS_Halibut_with_bow_thruster.jpg.
[49] Anna Borshchevskaya, "The Soviets' Unbreakable Code," Foreign Policy, 27 de abril del 2019, https://foreignpolicy.com/2019/04/27/the-soviets-unbreakable-code-fialka-encryption-espionage-russia-kgb-spy/.
[50] Daniel R. Headrick, The Invisible Weapon, capítulo 4.
[51] Sherry Sontag, Christopher Drew, and Annette Lawrence Drew, Blind Man's Bluff: The Untold Story of American Submarine Espionage (New York: Public Affairs, 1998), 222.
[52] Ibíd.
[53] Ibíd., 223.
[54] Ibíd.
[55] Matt Blitz, "Navy Divers and Their Daredevil Mission to Spy on the Soviet Union at the Bottom of the Sea," Popular Mechanics, 30 de marzo del 2017, https://www.popularmechanics.com/technology/security/a25857/operation-ivy-bells-underwater-wiretapping/.
[56] Michael J. Sulick, American Spies: Espionage Against the United States from the Cold War to the Present (Washington, DC: Georgetown University Press, 2013), 109–14; Matt Blitz, "Navy Divers."
[57] Damien McGuinness, "How a Cyber Attack Transformed Estonia," BBC News, 27 de abril del 2017, https://www.bbc.com/news/39655415; Rain Ottis, "Analysis of the 2007 Cyber Attacks Against Estonia From the Information Warfare Perspective," (Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2008), https://ccdcoe.org/library/publications/analysis-of-the-2007-cyber-attacks-against-estonia-from-the-information-warfare-perspective/.
[58] David Hollis, "Cyberwar Case Study: Georgia 2008," Small Wars Journal, 6 de enero del 2011, https://smallwarsjournal.com/jrnl/art/cyberwar-case-study-georgia-2008; Ronald J. Deibert, Rafal Rohozinski, and Masashi Crete-Nishihata, "Cyclones in cyberspace: Information shaping and denial in the 2008 Russia–Georgia war," Security Dialogue 43, No. 1 (2012): 3–24, https://journals.sagepub.com/doi/10.1177/0967010611431079.
[59] Pavel Polityuk and Jim Finkle, "Ukraine Says Communications Hit, MPs Phones Blocked," Reuters, 4 de marzo del 2014, https://www.reuters.com/article/us-ukraine-crisis-cybersecurity/ukraine-says-communications-hit-mps-phones-blocked-idUSBREA231R220140304; Sergey Sukhankin, "Russian Electronic Warfare in Ukraine: Between Real and Imaginable," Jamestown Foundation, 24 de mayo del 2017, https://jamestown.org/program/russian-electronic-warfare-ukraine-real-imaginable/.
[60] Andy Greenberg, "How an Entire Nation Became Russia's Test Lab for Cyberwar," Wired, 20 de junio del 2017, https://www.wired.com/story/russian-hackers-attack-ukraine/; "Six Russian GRU Officers Charged in Connection

with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace," Departamento de Justicia de Estados Unidos, 19 de octubre del 2020, https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and.

[61] Constanze Stelzenmüller, "The impact of Russian interference on Germany's 2017 elections," (testimonio congresional, 28 de junio del 2017), https://www.brookings.edu/testimonies/the-impact-of-russian-interference-on-germanys-2017-elections/.

[62] Maggie Miller, "US intel agencies blame Russia for massive SolarWinds hack," *The Hill,* 5 de enero del 2021, https://thehill.com/policy/cybersecurity/532756-us-intel-agencies-blame-russia-for-massive-solarwinds-hack.

[63] "Connect the Dots on State-Sponsored Cyber Incidents - Titan Rain," Council on Foreign Relations, https://www.cfr.org/cyber-operations/titan-rain.

[64] Garrett Graff, "China's Hacking Spree Will Have a Decades-Long Fallout," Wired, 11 de febrero del 2020, https://www.wired.com/story/china-equifax-anthem-marriott-opm-hacks-data/.

[65] Chun Han Wong, "China Launches Initiative to Set Global Data-Security Roles," *The Wall Street Journal,* 8 de septiembre del 2020, https://www.wsj.com/articles/china-to-launch-initiative-to-set-global-data-security-rules-11599502974.

[66] Bojan Pancevski, "U.S. Officials Say Huawei Can Covertly Access Telecom Networks," The Wall Street Journal, 12 de febrero del 2020, https://www.wsj.com/articles/u-s-officials-say-huawei-can-covertly-access-telecom-networks-11581452256.

[67] Joe Parkinson, Nicholas Bariyo, and Josh Chin, "Huawei Technicians Helped African Governments Spy on Political Opponents," The Wall Street Journal, 12 de agosto del 2019, https://www.wsj.com/articles/huawei-technicians-helped-african-governments-spy-on-political-opponents-11565793017.

[68] William Turton, "Hidden Back Door Embedded in Chinese Tax Software, Firm Says," Bloomberg, 25 de junio del 2020, https://www.bloomberg.com/news/articles/2020-06-25/hidden-back-door-embedded-in-chinese-tax-software-firm-says.