Laura Hochla

Originaria de Albuquerque, Nuevo México, se licenció en Economía por el Wellesley College, tiene un título de máster por la Universidad de Harvard y fue becaria Fulbright en Granada.

Laura Hochla ingresó en el Servicio Exterior de Estados Unidos en enero de 2006 y desde entonces ha estado destinada en Kosovo, Colombia, Georgia, España y la Oficina de Asuntos Rusos en Washington D.C. Con anterioridad, fue profesora de español.

Consejera Adjunta para Asuntos Económicos. Embajada de Estados Unidos

La tecnología 5G ante EL GRAN DESAFÍO DE LA SEGURIDAD

Laura Hochla

1 *¿Qué es la 5G y qué significará para mí?*

Todo lo que se diga sobre la transformación radical de nuestras vidas a causa de la tecnología 5G es poco. Muchos de los objetos comunes con los que ahora interactuamos estarán conectados, enviando y recibiendo información constantemente para ser más eficientes, utilizar menos energía o protegernos. Los vehículos autónomos reciben mucha atención en los medios y, sí, están llegando. Pero la baja latencia de la 5G —el tiempo que los datos tardan en llegar desde que son enviados— en la nueva Internet de las cosas significa que todo, desde nuestros dispositivos personales hasta nuestro frigorífico y nuestras gafas, puede estar —y probablemente estará— conectado. Esto traerá consigo un mundo completamente nuevo de aventura, innovación y cambio. Pero también lo llenará de amenazas, vulnerabilidades y riesgos. Existe, por supuesto, el riesgo para la ciberseguridad, la preocupación habitual por los piratas informáticos y las puertas de atrás. Pero existen también puertas principales que pueden quedar abiertas de par en par, invitando a nuevos niveles de robo de datos. Todas las cosas conectadas en red con las que interactuamos, o que interactúan con nosotros, crearán una gran cantidad de datos. Estos datos, que contendrán información sobre nosotros, también revelarán cómo, cuándo, dónde y con quién hacen negocios las empresas españolas: una información comercial muy valiosa. Podemos pensar que no tenemos nada que ocultar. Y tal vez los datos de un individuo no brinden a un gobierno extranjero hostil mucho con lo que trabajar. Pero si rastreamos los hábitos de una ciudad entera o incluso una sola terminal de contenedores, tendremos un tesoro de datos que podrían ser utilizados contra una compañía que compite por un contrato o un gobierno que está en mitad de una negociación. La tecnología también falla y el *software* necesita parches. Las entidades en las que elegimos confiar para que nuestra tecnología esté segura —encontrando vulnerabilidades y poniendo parches— resultan fundamentales para la seguridad personal, corporativa e incluso nacional.

2 ¿Por qué está tan preocupado Estados Unidos?

Las redes y los servicios son objetivos atractivos para los adversarios extranjeros y otros agentes nocivos. Dado el carácter global de los flujos de datos, las amenazas a las redes de Estados Unidos son amenazas para nuestros aliados, del mismo modo que las amenazas a las redes de nuestros aliados tienen una relación directa con la seguridad de Estados Unidos. Es muchísimo lo que está en juego, para todos nosotros, si no salvaguardamos nuestras redes críticas.

Estados Unidos quiere asegurarse de que tanto nosotros como nuestros socios y aliados mantenemos redes de comunicación y cadenas de suministro seguras y fiables para reducir los riesgos de un acceso no autorizado y una ciberactividad maliciosa. Esto es especialmente cierto en el ámbito del intercambio de inteligencia.

Dado que habrá componentes inteligentes realizando operaciones informáticas en toda la red, debemos garantizar su protección, desde el *core* a la periferia, y que no la contaminamos con elementos que no son fiables. Proteger solo los llamados "componentes principales" o *core* de la red 5G no es suficiente; dejar cualquier componente de la tecnología 5G a proveedores no fiables introduce riesgos innecesarios en la red y podría comprometer el intercambio de inteligencia de Estados Unidos con socios y aliados como España. Por eso estamos instando a nuestros socios a garantizar que los proveedores no fiables queden por completo fuera de sus redes 5G.

3 ¿Cómo está construyendo y protegiendo sus redes Estados Unidos?

Para proteger las redes estadounidenses, el 15 de mayo de 2019, el presidente Trump firmó la Orden Ejecutiva sobre la "Protección de la tecnología de la información y las comunicaciones y la cadena de suministro de servicios". Esta Orden Ejecutiva permite al Secretario de Comercio prohibir las operaciones que incluyen tecnología de las comunicaciones y la información que pueda estar controlada por un adversario extranjero o sujeta a su jurisdicción y que represente un riesgo inaceptable para nuestra seguridad nacional.

A partir del 1 de agosto de 2020 las conexiones 5G a todas las embajadas y consulados estadounidenses en todo el mundo tendrán que atravesar un "camino limpio" o "clean path" —una red sin componentes de suministradores de países autocráticos

En marzo de este año, el Congreso de Estados Unidos aprobó, sin oposición, y el presidente promulgó la "Ley de seguridad de la 5G y más allá". El gobierno de Estados Unidos también lanzó una estrategia nacional para proteger y ampliar el acceso a las redes de telecomunicaciones de Estados Unidos.

También en marzo, el presidente firmó la "Ley de redes de comunicaciones seguras y fiables", que prohíbe que ciertos préstamos, subvenciones y subsidios federales sean utilizados para adquirir u obtener equipos o servicios de comunicaciones que presenten riesgos para la seguridad nacional. Además, mediante esta ley se financia la sustitución de los equipos no fiables utilizados actualmente en las redes de Estados Unidos. Asimismo, el presidente firmó la "Ley de datos de banda ancha", que mejorará los mapas de la cobertura de banda ancha de la Comisión Federal de Comunicaciones (FCC, por sus siglas en inglés) ayudando a garantizar que la financiación se centre más en las zonas que actualmente carecen de servicio. Esto contribuirá a los esfuerzos para dar conexión a los estadounidenses en todo el país.

En abril, el secretario de Estado, Mike Pompeo, anunció que a partir del 1 de agosto de 2020 las conexiones 5G a todas las embajadas y consulados estadounidenses en todo el mundo tendrán que atravesar un "camino limpio" o "clean path" —una red sin componentes de suministradores de países autocráticos—.

Estas medidas cuentan con un amplio apoyo de los dos partidos en Estados Unidos. Tanto los demócratas como los republicanos reconocen que nuestra infraestructura de TI es crítica. Y estas medidas no apuntan a ningún país o empresa: están diseñadas para garantizar que nuestras redes sean construidas con y por compañías fiables no sujetas a las leyes de gobiernos antidemocráticos y autoritarios.

Sede central de Huawei en Shenzhen, China.

4 ¿Cuál es el problema con el hardware de fabricación china?

La Ley de seguridad nacional de China, la Ley de contraespionaje, la Ley de inteligencia nacional, la Ley contra el terrorismo, la Ley de ciberseguridad y otros mecanismos conceden al gobierno chino poderes amplios y difusos que obligan a los proveedores de telecomunicaciones y de servicios en línea con sede en China o que operen allí a proporcionar acceso a los servicios de inteligencia y seguridad chinos y a cooperar con ellos. En resumen, cualquier empresa china debe colaborar con el gobierno chino, por lo que incluir a dichos proveedores en una red significa incluir también al gobierno chino.

La amenaza que nos preocupa especialmente es el amplio alcance extraterritorial de la Ley de seguridad nacional de China de 2017. China ha desarrollado rápidamente un marco legislativo para aumentar su control sobre los datos, las redes y la información en el ciberespacio.

Además, según la ley china, las autoridades pueden realizar revisiones de seguridad invasivas, exigir a las empresas que localicen y desencripten datos, que entreguen el código fuente u otra información sensible y confidencial, y que proporcionen asistencia técnica para dar cumplimiento a las solicitudes de los organismos de seguridad o a los requerimientos de vigilancia y censura. Y aquí está la clave: estas obligaciones pueden extenderse a los datos que están en poder de las empresas sujetas a la ley china fuera de sus fronteras o que son accesibles a ellas.

El Artículo 9 de la Ley de seguridad nacional de China establece que "para el mantenimiento de la seguridad nacional […] los ciudadanos y las organizaciones serán ampliamente movilizados para evitar, frustrar y castigar legalmente cualquier conducta que comprometa la seguridad nacional".

En otras palabras, no obedecer no es una opción para empresas como Huawei o ZTE. La coacción y los instrumentos legales de China se aplican tanto a las empresas estatales como a las aparentemente privadas. Ninguna goza de un recurso legal realista para oponerse a las directivas del gobierno chino. A diferencia de lo que ocurre en democracias como Estados Unidos y España, el sistema judicial chino no es independiente y seguirá la dirección del Partido Comunista Chino. El presidente Xi ha declarado abiertamente que China no caminará por la senda occidental de la separación de poderes constitucional, con un poder judicial independiente.

Esto es más que un simple análisis teórico de la legislación china. Ya hemos visto a empresas tecnológicas chinas colaborar con el gobierno chino para suprimir la libertad de expresión y los derechos humanos. Lo hacen a través de una vigilancia arbitraria, censura y restricciones específicas al acceso a Internet.

Este mal uso y abuso del acceso y de los datos, por supuesto, también ocurre en el mundo de los negocios. El representante de Estados Unidos para el Comercio confirmó recientemente que, durante más de diez años, el gobierno chino ha realizado y respaldado ciberataques a las redes comerciales de Estados Unidos, apuntando a información empresarial confidencial en poder de empresas estadounidenses.

También sabemos que China estaba detrás de uno de los mayores robos de información de compañías en diciembre de 2018. Lo que se conoció como "ataques Cloud Hopper" fueron ataques del Ministerio de Seguridad del Estado chino que comprometieron a proveedores de servicios administrados globalmente y de servicios en la nube. Ello les dio acceso a redes enteras de información de grandes empresas. Parte de esa información fue suministrada después a compañías chinas para darles ventaja sobre sus competidores comerciales.

Huawei ha sostenido que no estaría obligada por la Ley de inteligencia nacional china a cumplir los mandatos del Partido Comunista de China y del Estado chino, aunque no hay forma de oponerse. Los servicios de seguridad chinos ya están infiltrados y es de conocimiento público que hay empleados de Huawei con estrechos vínculos con el Ejército Popular de Liberación, las fuerzas armadas de China, y los servicios de inteligencia. Ha habido investigaciones que detallaban las subvenciones masivas que Huawei ha recibido del gobierno chino a lo largo de los años. No solo hay control legal del gobierno chino, también hay control financiero.

Las vulnerabilidades técnicas en los productos de Huawei aumentan más el riesgo. En 2019, la Junta de Supervisión de Huawei en el Reino Unido descubrió que había cientos de vulnerabilidades en los productos de Huawei. Además, determinó que hubo defectos graves y sistemáticos en la ingeniería del *software* y la capacidad de la ciberseguridad de Huawei.

Estos hallazgos fueron respaldados recientemente por la empresa de ciberseguridad Finite State en Estados Unidos, que estudió el *firmware* de varios dispositivos Huawei, lo que reveló una protección de ciberseguridad de calidad inferior a la ofrecida por sus competidores. De hecho, la compañía descubrió que había contraseñas de codificación fija y prácticas criptográficas inseguras en el propio *firmware*.

Estas vulnerabilidades en conjunto equivalen no solo a una puerta de atrás sino a una puerta principal.

Estados Unidos no cree únicamente que compañías como Huawei y ZTE representan amenazas importantes para las redes de comunicaciones debido a sus vínculos con los servicios de seguridad chinos y a las leyes chinas que deben acatar. Nos preocupa también cualquier compañía que muestre su disposición a violar las leyes estadounidenses.

A Estados Unidos también le preocupa que haya compañías que violan sus leyes descaradamente. En 2019

y 2020, el departamento de Justicia de Estados Unidos ha emitido acusaciones relacionadas con la conspiración deliberada de Huawei para robar propiedad intelectual estadounidense, incluyendo de T-Mobile US, en un intento por socavar los mercados mundiales libres y justos. En el caso de T-Mobile, Huawei robó información sobre un robot de prueba de teléfonos T-Mobile con el fin de tratar de construir su propio robot para probar los teléfonos antes de enviarlos a T-Mobile y otros operadores de telefonía móvil. Los ingenieros de Huawei violaron los acuerdos de confidencialidad y no revelación de información con T-Mobile al tomar fotos del robot y medidas de partes del robot a escondidas y, en una ocasión, incluso robar una pieza del robot para que los ingenieros de Huawei en China pudieran tratar de replicarlo.

Después de que T-Mobile descubriera e interrumpiera estas actividades delictivas y amenazara con una demanda, Huawei afirmó falsamente que el robo había sido obra de actores corruptos dentro de la empresa y no un esfuerzo concertado de las entidades corporativas de Huawei en Estados Unidos y China. La investigación posterior reveló que la conspiración para robar secretos de T-Mobile fue un esfuerzo de toda la compañía que involucró a muchos ingenieros y empleados. Huawei incluso ofreció primas a los empleados en función del valor de la información robada a otras compañías en todo el mundo.

5 Inclusión en la Lista de entidades de Estados Unidos

En mayo de 2019, Estados Unidos dio un paso importante para asegurar sus redes y su tecnología al añadir a Huawei a la Lista de entidades restringidas. Huawei fue incluida en dicha lista debido a los años de suministro de equipos de telecomunicaciones a Irán —en violación de las sanciones internacionales— y su actitud engañosa sobre dicha práctica.

Sin embargo, tras ser incluida en la Lista de entidades en 2019, Huawei ha continuado utilizando *software* y tecnología de Estados Unidos para diseñar semiconductores, lo que socava el propósito de la Lista de entidades en relación con la seguridad nacional y la política exterior, ya que encargó su producción en plantas fuera del país utilizando equipos estadounidenses.

Por este motivo, el 15 de mayo de 2020, el departamento de Comercio de Estados Unidos anunció planes para proteger la seguridad nacional de Estados Unidos restringiendo la capacidad de Huawei para utilizar tecnología y *software* estadounidenses en el diseño y fabricación de sus semiconductores en el extranjero. Este anuncio cercenó los esfuerzos de Huawei por socavar los controles a la exportación por parte de Estados Unidos. La Oficina de Industria y Seguridad del Departamento de Comercio modificó su normativa sobre productos directos producidos en el extranjero y la Lista de entidades, para centrarse atenta y estratégicamente en la adquisición, por parte de Huawei, de semiconductores que sean producto directo de ciertos *software* y tecnología estadounidenses.

La conspiración para robar secretos de T-Mobile fue un esfuerzo de toda la compañía que involucró a muchos ingenieros y empleados. Huawei incluso ofreció primas a los empleados en función del valor de la información robada a otras compañías en todo el mundo

6 Es posible construir una red 5G sin China

Estados Unidos está construyendo una red 5G utilizando *hardware* fabricado por Ericsson, Nokia y Samsung. Es absolutamente posible construir una red de primer nivel sin proveedores de países autocráticos. El hecho de que Estados Unidos esté construyendo una red 5G de vanguardia que ya opera en ciudades clave contradice la premisa de que el equipo de Huawei es de alguna manera superior al de otros proveedores.

Ericsson, Nokia y Samsung tienen los componentes que necesitan para proporcionar el mismo

A principios de 2020, el gobierno español anunció con prudencia que desarrollaría un comité de revisión para analizar los riesgos de los proveedores de tecnología 5G

nivel de funcionalidad que Huawei y los proveen a empresas en todo el mundo —también en Europa— para que ofrezcan la tecnología punta 5G. Y, de hecho, cuando abrimos las estaciones base, los componentes clave, es decir, los componentes clave de los microprocesadores, proceden de compañías como Qualcomm.

7 Colaboración con nuestros aliados en Europa

El Consejo de la Unión Europea dejó claro en enero de este año que, además de analizar los riesgos para la seguridad técnica de los proveedores de tecnología 5G, los países deben abordar factores no técnicos como los marcos legislativos y las políticas de los proveedores que se rigen por los países donde tienen su sede central. A principios de 2020, el gobierno español anunció con prudencia que desarrollaría un comité de revisión para analizar los riesgos de los proveedores de tecnología 5G.

Esos factores no técnicos se deben abordar porque cualquier tecnología basada en *software* se puede actualizar instantáneamente. Tales actualizaciones pueden incluir riesgos o vulnerabilidades. Resulta sencillamente imposible que cualquier ser humano revise las decenas de millones de líneas de código para identificar siquiera una que pueda ser la causa de una interrupción en la red o permitir la filtración no autorizada de datos.

Además, el Consejo de la UE señaló que la estandarización y la certificación por sí solas no serán suficientes para proteger las redes 5G.

Estados Unidos está de acuerdo con la Unión Europea en que necesitamos generar confianza en el 5G y proteger los valores comunes, como son los derechos humanos, el estado de derecho, la privacidad, los derechos de propiedad intelectual y la transparencia.

Una pieza clave de la Estrategia Nacional de Estados Unidos para proteger la 5G se centra en la cooperación con los aliados. La estrategia establece que Estados Unidos trabajará con países con ideas afines para liderar el desarrollo y la implantación de la tecnología 5G internacionalmente de manera responsable y promoverá la disponibilidad en el mercado de equipos y servicios seguros y fiables. También señala que el gobierno de Estados Unidos participará en el desarrollo de principios internacionales de seguridad 5G a través de marcos como la Conferencia sobre la Seguridad de la 5G celebrada en Praga en mayo de 2019, que dio lugar a las Propuestas de Praga: un conjunto de factores que los países considerarán al determinar cómo proteger la infraestructura sensible de la tecnología de la información.

Otra área en la que estamos cooperando estrechamente con España y otros aliados gira en torno a los estándares. Estamos trabajando con organizaciones relevantes que establecen los estándares de acuerdo con el sector privado como, entre otros, socios comerciales, académicos e internacionales con ideas afines. Continuamos subrayando la necesidad de procesos abiertos y transparentes para desarrollar estándares oportunos, técnicamente sólidos y apropiados.

El sector privado es un socio clave en esta tarea, en Europa y en Estados Unidos. El gobierno de Estados Unidos trabaja con el sector privado, el mundo académico y gobiernos internacionales para adoptar políticas, estándares, directrices y estrategias de compra que refuercen la diversidad de los proveedores de tecnología 5G, fomentando así la competencia en el mercado. Junto con el sector privado y nuestros socios internacionales diseñaremos incentivos basados en el mercado, mecanismos de rendición de cuentas y procedimientos de evaluación de la diversidad, la transparencia de los componentes, la financiación justa y la competencia

en todo el panorama de la tecnología 5G como medio para proteger mejor la red mundial y nuestros valores compartidos de apertura, seguridad e interoperabilidad.

8 *Las decisiones que tomemos ahora garantizarán la seguridad durante décadas*

Al construir la infraestructura 5G hoy, debemos considerar no solo el riesgo tecnológico, sino también el relacionado con los socios en los que decidimos confiar. Estados Unidos y Europa comparten los mismos valores fundamentales, como el respeto por la privacidad y el debido proceso. Estados Unidos está con Europa y España en la defensa de esos valores, no solo en el mundo físico, sino también en el mundo digital.

El Consejo de la UE señaló que la estandarización y la certificación por sí solas no serán suficientes para proteger las redes 5G