CONFRONTACIÓN ESTADOS UNIDOS-CHINA: DE GEOPOLÍTICA, TECNOLOGÍA Y RIESGOS PARA NUESTRA REGIÓN

Irene Levy, Mauricio Meschoulam y Michel Hernández

Agradecemos al equipo del Centro de Investigación para la Paz México, AC. por su colaboración en la preparación de este trabajo

RESUMEN EJECUTIVO Y PRINCIPALES CONCLUSIONES

1. *Contexto: el enfrentamiento geopolítico EEUU - China*

El enfrentamiento entre Estados Unidos y China no consiste únicamente en la competencia material entre dos grandes potencias. Se trata también de la relación entre una potencia que se autopercibe en crecimiento y expansión y que percibe a la otra como decadente, frente a ese otro superpoder que parece estarse percibiendo a sí mismo como fuerte, pero rezagado, y con la necesidad de recuperar el terreno perdido.

Sin embargo, la interdependencia que se vino construyendo históricamente entre ambos países hace que sea imposible cortar de tajo la vinculación económica y tecnológica existente. Dicha vinculación produce intereses muy diversos, no todos los cuales se encuentran caminando en una misma dirección. Hoy se plantea en Washington la necesidad de desvincular a ambas economías, o al menos de hacerlas menos interdependientes. Todo lo anterior está detonando una dinámica propia marcada por un conflicto ascendente que se manifiesta de múltiples formas.

La competencia entre potencias ya no es exclusivamente militar. Existe un abanico mucho mayor de ámbitos en los cuales los países rivalizan, como el campo de la tecnología o la información. El contexto actual es muy diferente al de la Guerra Fría o al de los sistemas de competencia del pasado.

La administración Trump ha dado un viraje en la concepción de la seguridad nacional estadounidense. La Estrategia de Seguridad Nacional del 2017 y la Estrategia de Defensa Nacional en 2018 marcan el cambio al reconocer la "competencia estratégica" entre las potencias—y no el terrorismo—como la mayor de las amenazas a Estados Unidos. Dada su capacidad económica, militar y tecnológica, y su proyección hacia el largo plazo, China es percibida como una mayor amenaza que Rusia.

La rivalidad China-Estados Unidos se despliega en muchos terrenos, de los cuales la tecnología forma parte fundamental. Para algunos sectores dentro del gobierno de Estados Unidos, China utiliza el endeudamiento de otros países, el comercio, la inversión y sus lazos económicos para avanzar sus propios intereses, lo que incluye el robo de tecnología, investigación, desarrollo e innovación o la presión en contra de diversos gobiernos, incluidos algunos latinoamericanos, para alinearse con la visión geopolítica y estratégica de Beijing.

2. *La polémica en torno a las empresas tecnológicas chinas*

El surgimiento de China como potencia en tecnologías de la información y la comunicación, principalmente representada por el ascenso de Huawei y su posición en el mapa mundial de las telecomunicaciones, ha generado temores, acusaciones y bloqueos en Estados Unidos.

El posicionamiento de Huawei en el mapa mundial de las telecomunicaciones ha sido objeto de controversia y diversos cuestionamientos, originados principalmente en Estados Unidos, en 4 aspectos fundamentales: (i) apoyo financiero del gobierno chino; (ii) disputas sobre derechos de propiedad intelectual; (iii) estrechos vínculos de la empresa con el ejército chino; y (iv) amenazas a la seguridad nacional de Estados Unidos.

También es motivo de polémica la existencia de un "Comité del Partido Comunista" en la empresa, que ha sido defendido bajo la justificación de la necesaria moralidad y responsabilidad social entre los líderes de la compañía.

Uno de los principales temores en Estados Unidos sobre la inmersión de Huawei—y, en general, de las empresas tecnológicas chinas—en sus mercados internos, es la amenaza a la seguridad nacional que supondría el uso de sus tecnologías y equipos con fines distintos a los meramente comerciales. Dicho de otra forma: el temor a que empresas como Huawei sean un medio para el espionaje o sabotaje que estaría impulsado por el gobierno chino, particularmente ante el inminente auge de la tecnología 5G.

3. ¿Qué han hecho otros países al respecto?

Reino Unido creó desde 2010 un "Centro de Evaluación de la Ciberseguridad de Huawei" ("HCSEC" por sus siglas en inglés), a partir de una serie de acuerdos entre la empresa y el gobierno británico, con la finalidad de mitigar cualquier riesgo que se perciba derivado del involucramiento de Huawei en aspectos de la infraestructura crítica nacional del Reino Unido. Dicho órgano concluyó que se han identificado cuestiones técnicas relevantes en los procesos de ingeniería de Huawei que representan nuevos riesgos para las redes de telecomunicaciones.

La Unión Europea recomendó que, a nivel nacional, los estados deberían realizar para finales de junio de 2019 una evaluación de riesgos en relación con las infraestructuras de red de 5G. La Comisión Europea recomendó una serie de acciones operativas y medidas para garantizar un alto nivel de ciberseguridad de las redes 5G, el cual parte de una resolución del Parlamento Europeo aprobada el 12 de marzo de 2019 sobre amenazas a la seguridad relacionadas con el crecimiento de la presencia tecnológica china.

Nueva Zelanda, a través de su agencia de inteligencia, rechazó en noviembre de 2018 la solicitud de Spark New Zealand Ltd., proveedor de servicios de telecomunicaciones, de emplear equipos de tecnología 5G de la compañía china Huawei, bajo argumentos de seguridad nacional.

Australia prohibió en agosto de 2018 la participación de Huawei en la construcción de redes 5G en ese país, argumentando también razones de seguridad nacional, al señalar que "el involucramiento de fabricantes que podrían estar sujetos a instrucciones extrajudiciales de un gobierno extranjero, en conflicto con la legislación Australiana, podrían poner en riesgo a los proveedores de servicios de fallar en la adecuada protección de las redes 5G de cualquier intervención o acceso injustificado".

Japón prohibió en diciembre de 2018 el uso de determinados equipos en las adquisiciones del sector público, con la finalidad de evitar fugas de información sensible derivadas de funcionalidades con intención maliciosa. Aunque las disposiciones implementadas no mencionan específicamente a alguna empresa, las más afectadas fueron Huawei y ZTE.

4. América Latina

La participación de las empresas tecnológicas chinas en América Latina cobra cada vez mayor relevancia dentro de ese entorno de competencia geopolítica. La expansión de las inversiones chinas en nuestro continente es frecuentemente percibida entre los sectores más duros en Estados Unidos como abiertos intentos para incrementar la influencia china en una órbita que Washington considera de influencia exclusiva: el hemisferio occidental.

En América Latina, la discusión sobre ciberseguridad no ha madurado tanto como en otras regiones del mundo. Los esfuerzos de protección en la materia son apenas esbozos, en muchos casos desarticulados, tanto internamente como hacia el exterior.

Al mismo tiempo, la inversión de empresas de origen chino en esta zona continúa incrementándose y el mercado es todavía muy amplio.

En materia de ciberseguridad, los datos muestran que **la región latinoamericana todavía no cuenta con la fortaleza necesaria:**

- En 2017 América Latina sufrió 667 millones de ciberataques, 57% más que en el año anterior, lo que le costó a la región $97 billones de dólares.
- En el mismo año, México fue el tercer país del mundo que recibió más ciberataques y el primer lugar de América Latina, lo que reflejó una pérdida de 7,700 millones de dólares.

América Latina está en una situación de vulnerabilidad muy particular, si asumimos que las amenazas que se han planteado en Estados Unidos y otros países en el uso de equipos chinos son reales.

Si los riesgos para países más industrializados siguen siendo enormes, aunque han tomado medidas preventivas desde hace años, pensemos qué sucede en países y sociedades como las de nuestro subcontinente, que mayormente carecen de la preparación para resistir ese tipo de vulnerabilidades, las cuales tienden a potenciarse bajo condiciones de corrupción e impunidad.

El control de las redes de comunicación e información no es un tema menor. Los reportes y señales que apuntan hacia el uso de la tecnología para avanzar determinados intereses estratégicos en el medio de una disputa mayor, se siguen sumando.

5. Principales conclusiones

La presencia de tecnología china en el despliegue y operación de redes de telecomunicaciones, particularmente 5G, implica riesgos a la seguridad nacional. Sin embargo, lo mismo podría decirse de cualquier otro gobierno o país que se involucre directamente en este despliegue. Cualquier medida al respecto debe ser adoptada considerando las particularidades de los proveedores y las vulnerabilidades identificadas en el país que corresponda.

México ocupa una posición estratégica en la disputa entre EEUU y China. Nuestro país debe ser sumamente cauteloso pues hay algunos valores fundamentales involucrados que pudieran verse comprometidos a cambio de una ventaja o apalancamiento comercial de parte de China, como la seguridad, la privacidad, los datos personales e, incluso, la propia relación con Estados Unidos.

No se observa a la fecha que la ciberseguridad sea un tema que se encuentre en el centro de la agenda pública en México. Las principales discusiones en el país en materia de despliegue de redes 5G en México se han centrado en aspectos comerciales; hasta ahora, el componente de seguridad nacional aparece de manera muy marginal.

6. Recomendaciones

La presencia y expansión de empresas tecnológicas chinas es una realidad y deben tomarse acciones. México no debe "esperar y ver" lo que sucede en otros países en materia de seguridad nacional ante la presencia de tecnologías chinas en el despliegue de redes de telecomunicaciones.

México podría evaluar la pertinencia de hacer algo similar a lo sucedido en Reino Unido con el HCSEC. Esto significaría adoptar un enfoque de participación de múltiples partes (*multistakeholder*) para atender las cuestiones relacionadas con presencia tecnológica china en México. Una aproximación basada en riesgos pudiera ser la más apropiada para atender los cuestionamientos derivados de la presencia y expansión tecnológica de China en nuestro país.

En la discusión sobre redes 5G, el componente de seguridad nacional debe ser considerado con una política de Estado. Esto con independencia de las empresas que pueden ofrecer equipos para la operación de dichas redes.

Debe tomarse en cuenta lo establecido en el artículo 6 de la Constitución mexicana. Ahí ya se establece como principio de política pública la prohibición de injerencias arbitrarias en la prestación de servicios de telecomunicaciones. Este principio se debe hacer valer por las autoridades en México.

Deben definirse las tareas de cibserseguridad necesarias para el país y establecer la autoridad o autoridades que estarán a cargo de dichas labores de manera articulada. Por lo pronto, no nos pronunciamos sobre el modelo institucional más apropiado pues deben analizarse diversos factores, pero es necesario iniciar la discusión cuanto antes.

Sería necesaria la coordinación regional. Ante el contexto internacional, el tema de ciberseguridad, particularmente en redes 5G, puede ser uno que se atienda mejor de manera regional, ya que los países latinoamericanos comparten características comunes que podrían propiciar acciones y posiciones coordinadas en beneficio de todos.

Es urgente que se analice la creación de un marco jurídico en materia de ciberseguridad. Este debe ser uniforme y aplicable en todos los niveles de gobierno, sin que ello implique límites rígidos a la innovación o el desarrollo de los mercados.

CONFRONTACIÓN ESTADOS UNIDOS-CHINA: DE GEOPOLÍTICA, TECNOLOGÍA Y RIESGOS PARA NUESTRA REGIÓN

Introducción

En noviembre del 2018, durante el Foro de Seguridad Internacional de Halifax, Canadá, se pudo apreciar, varias veces, un reconocimiento abierto por parte de distintos militares estadounidenses: de no revertir la tendencia actual a partir de un significativo incremento en inversión para investigación y desarrollo tecnológico, Washington vería su poder relativamente disminuido ante Rusia y, sobre todo, ante China. Uno de los autores de este texto tuvo oportunidad de preguntar al General Dunford, el Jefe del Estado Mayor Conjunto de los Estados Unidos si, en su visión, Washington se había descuidado demasiado en los últimos años debido a su alta concentración de esfuerzos para combatir a Al Qaeda y a ISIS. Dunford respondió que era muy difícil efectuar juicios sobre el pasado, pero que, visto a la distancia, él quizás sí habría decidido diferente.

Esa es solo una muestra de lo que parece ser una percepción generalizada. La carrera entre las superpotencias, especialmente entre Estados Unidos y China, está corriendo a toda velocidad, lo que puede ser observado en muy distintos rubros. Se trata de temas que aparecen de manera salteada en las noticias de todos los días. Un día se nos cuenta acerca de la expansión de China en sus mares colindantes y acerca de cómo un buque de guerra estadounidense que, desafiando zonas marítimas que China reclama como suyas, participaba en una de las expediciones de "libertad de navegación", y al ser asechado por un navío chino, tuvo que maniobrar para no colisionar. Otro día se habla acerca de las ventas de armas de Washington a Taiwán. Luego, cuando apenas vamos digiriendo los sube y bajas de la guerra comercial, Beijing acusa a Washington de instigar las manifestaciones en Hong Kong. No pasan unas horas cuando se habla sobre la injerencia de Beijing en redes sociales con cuentas falsas en temas políticos o electorales o sobre las prohibiciones a Huawei y las medidas que esta empresa china está tomando para asegurar su futuro. El problema es que, ante semejante torbellino de noticias, es fácil extraviarse y omitir el panorama mayor: la actual relación entre las dos máximas potencias del globo, EEUU y China, es el resultado de una combinación de factores, unos de los cuales les obligan a cooperar, otros les llevan a competir y otros más les están llevando a un enfrentamiento estratégico de largo plazo.

El objetivo de este texto es mostrar cómo la actual confrontación tecnológica existente entre EEUU y China está funcionando como un componente más—uno de los mayores ciertamente—en ese enfrentamiento sistémico, y cómo es que, dentro de ese entorno de competencia geopolítica, la participación de las empresas tecnológicas chinas en espacios como nuestro propio continente, cobra cada vez mayor relevancia.

En palabras simples podríamos estar hablando del choque estructural provocado por un poder emergente—China—país que en la actualidad tiene la voluntad y se siente con la necesidad y las capacidades de ocupar cada vez mayores espacios en el plano global, y otro poder—Estados Unidos—que sigue superando al primero en términos militares,

económicos y tecnológicos, pero que ha estado dando importantes señales de declive relativo.

No se trata, entonces, solamente de la competencia material entre dos grandes potencias, sino de la relación resultante entre una potencia que se autopercibe en crecimiento y expansión y que percibe a la otra como decadente, frente a ese otro superpoder que parece estarse percibiendo a sí mismo como fuerte, pero rezagado, y con la necesidad de recuperar el terreno perdido.

No obstante, al abordar nuestro análisis, hablaremos también acerca de cómo esa relación entre ambas superpotencias es mucho más compleja de lo que a veces se plantea. La interdependencia que se vino históricamente construyendo hace que sea imposible, incluso si se quisiera, cortar de tajo la vinculación económica y tecnológica existente, lo que produce intereses muy diversos, no todos los cuales se encuentran caminando en una misma dirección.

Aún así, la situación actual arroja una serie de señales que parecen indicar que los objetivos estratégicos de estos dos superpoderes seguirán colisionando de manera cada vez más importante, lo que ocasionará que, de desear evitar una escalada que pudiese salirse de las manos y traducirse en un conflicto mayor, ambas potencias deberán encontrar nuevos parámetros y arreglos para su coexistencia pacífica. El argumento de este trabajo es que estamos apenas en los momentos de definición, y que, en este punto, las negociaciones comerciales y en materia tecnológica—marcadas por amenazas, por medidas ya puestas en marcha, por otras temporalmente suspendidas, por fases de diálogo, por promesas incumplidas, por el endurecimiento y el relajamiento de posiciones—forman parte de este macroproceso de definiciones. La suma tanto de los pasos que se tomen en los próximos meses y años para afianzarse dentro de esta competencia global, como de lo que resulte de sus conversaciones y arreglos, terminará por impactar en sus relaciones de largo plazo. De ahí la importancia de cada uno de los ámbitos que componen este enfrentamiento sistémico, como lo es la carrera por tener presencia tecnológica en América Latina.

En los siguientes párrafos abordaremos algunas de las formas como ese enfrentamiento se ha estado manifestando. En la primera parte de este trabajo, hablamos acerca de la naturaleza y la geopolítica del choque estructural entre China y EEUU, la interdependencia y las dificultades que conlleva destejer esa interdependencia, así como la evolución de la conflictiva a lo largo de los últimos años y meses en distintas esferas. La segunda parte aborda de manera más específica la dimensión tecnológica de la rivalidad, así como los riegos que ello presenta para nuestra región y en específico para México. El texto termina con algunas conclusiones y recomendaciones a partir de lo presentado.

Parte I: La naturaleza y la geopolítica del enfrentamiento EEUU-China

1. ¿Guerra Fría? ¿Competencia estratégica? ¿Rivalidad?

Entender la naturaleza del conflicto existente entre las dos mayores superpotencias del globo no es una cuestión banal; la conceptualización que se haga del mismo puede impactar las percepciones, los diagnósticos y las decisiones de política. Al respecto del tema se ha suscitado un amplio debate del cual, para efectos de este ensayo, solo a manera de introducción, recuperamos algunas líneas argumentativas.

Hablar de la "nueva era" de competencia entre "grandes poderes" se ha vuelto un lugar común. Las estrategias de Seguridad Nacional de EEUU de 2017 y la Estrategia de Defensa Nacional de EEUU en 2018 marcaron el giro: "*inter-state strategic competition, not terrorism, is now the primary concern in U.S. national security*," indicando que, habiendo siendo descartada a lo largo de los últimos años, esta *competencia estratégica* había "regresado". Diversos funcionarios y analistas en Washington utilizan esa terminología con frecuencia. Sin embargo, para autores como Mazarr (2018) se está cometiendo un error conceptual. Es decir, no significa que no se esté generando la competencia de la que se habla, sino que no debería denominarse de la misma forma como se ha denominado a fenómenos similares en el pasado ("Guerra Fría" o "Competencia entre grandes poderes") puesto que, en la visión de estos autores, estamos ante circunstancias muy diferentes:

a) A diferencia del pasado, el actual no es un sistema propiamente multipolar, dice Mazarr. EEUU cuenta con ventajas competitivas económicas y militares de tal magnitud, que hacen que la situación de los sistemas multipolares de otros momentos de la historia sea incomparable a las circunstancias del siglo XXI.

b) El actual sistema de instituciones, regulaciones y normas internacionales impone restricciones al comportamiento de los estados que nunca antes en la historia hubiésemos imaginado, y este es el entorno en el que la actual rivalidad entre las superpotencias se está gestando.

c) Por último, mientras que en el pasado las áreas de rivalidad eran esencialmente económicas y político-militares, hoy lo militar juega un rol diferente: menos como herramienta de guerra y mucho más como instrumento para disuadir o ejercer la coerción. En cambio, existe un mucho mayor abanico de esferas en las cuales los países rivalizan—como por ejemplo el campo de la tecnología o la información.

Empleando una línea argumentativa diferente, Odd Arne Westad (2019) indica que es fundamental comprender cual es la raíz de la conducta de China en el presente para no incurrir en concepciones equivocadas.

En efecto, para China el crecimiento y la acumulación de poder son fundamentales. En los discursos de Xi Jinping es posible detectar la concepción de que el modelo chino es una mejor alternativa que los occidentales no solo para esa potencia, sino para otros países. Hay también mensajes nacionalistas y una sensación implícita de las humillaciones del pasado. Sin embargo, de acuerdo con Westad, Beijing está buscando sobre todo un dominio a nivel regional, un espacio geográfico en donde sí es altamente competitiva con Washington.

Westad coincide con otros autores en que, a diferencia de la URSS durante la Guerra Fría, para China la rivalidad con Estados Unidos no es ideológica. De hecho, el capitalismo es un modelo económico que ha penetrado en China y que coexiste con el modelo comunista, lo que hace que la sociedad china de la actualidad se mucho más parecida a los EEUU en sus patrones de consumo y de comportamiento que lo que lo era la URSS en su época. Más aún, el Partido Comunista Chino, de acuerdo con Westad, es nacionalista, no internacionalista. Adicionalmente, para Beijing hay reglas y temas globales que no solo está dispuesta a asumir, sino en los que busca un relativo liderazgo como lo es la cuestión del cambio climático.

En todo caso, esta serie de autores parece coincidir en cuanto a que lo militar es hoy menos relevante que en el pasado y que la rivalidad entre estas dos superpotencias se desahoga en otro tipo de rubros como lo es el campo tecnológico.

Para sellar las diferencias de esta con otras etapas de la historia, las economías de las dos superpotencias se encuentran entretejidas como nunca sucedió entre la economía estadounidense y la soviética, o bien, en otros momentos de la historia, lo que hace que los riesgos de una guerra inmediata sean inferiores a los de otros tiempos, y que en cambio, las probabilidades de una cooperación—aunque fuese limitada—son mucho mayores.

Dicho lo anterior, a partir de nuestra propia postura, habría que efectuar las siguientes precisiones:

1) Efectivamente, en la actualidad hay lazos de interdependencia compleja (Keohane y Nye, 1977) entre China y EEUU que ocasionan que las relaciones entre ambas potencias no se limiten al conflicto, sino que incluyen necesariamente incentivos para la cooperación. Pero es precisamente por ello por lo que muchos estrategas en Washington argumentan la necesidad de tomar pasos firmes para desasociar a las economías y desempatar los intereses que actualmente son comunes. Eso haría más viable y creíble cualquier estrategia de enfrentamiento. Probablemente Trump no debería ser caracterizado como uno de estos estrategas de largo plazo, pero ciertamente su política de “America First” y su guerra comercial con Beijing viene a caer como “anillo al dedo” para todo ese sector de línea dura.

2) También es verdad que la rivalidad actual es mucho menos un enfrentamiento ideológico que geopolítico. Eso, sin embargo, como lo señalan los propios autores, no implica que la rivalidad o la competencia no existan o que no puedan adquirir su propia dinámica.

3) Es justo en ese punto cuando, más que pensar en paralelos con el pasado, lo esencial es comprender la dinámica propia de los conflictos, y de este conflicto en particular, el cual puede arrastrar a las partes a espirales ascendentes en medio de las cuales se vean forzadas a tomar decisiones y acciones no siempre previstas.

4) En ese sentido, coincidimos en cuanto a que lo militar puede hoy tener menos peso relativo, o quizás funciones distintas que en el pasado. No obstante, entender cómo opera la dinámica ascendente de los conflictos resulta fundamental para vislumbrar—y prevenir—escenarios dentro de los cuales tanto la confrontación en rubros no militares, como eventos que sí son propios de la rivalidad militar (como las carreras armamentistas)—los cuales no pueden ser del todo descartados—podrían llegar a activar escalamientos que hoy no parecen estar sobre la mesa.

Veamos entonces de donde procede y cómo funciona la asociación o "emparejamiento" económico del que hablamos.

2. Desvincular a las economías

Estados Unidos no solo contribuyó, sino que se convirtió en uno de los pilares fundamentales del crecimiento chino de 1980 hasta la fecha, pero menos como inversionista y más como consumidor de los bienes producidos en ese país. Esto obedeció inicialmente a las condiciones y evolución de la Guerra Fría, especialmente durante los años 70. Hacia esos años, la Casa Blanca consideró que el acercamiento estratégico con Beijing podía ser una jugada de largo plazo que contribuiría al ya existente distanciamiento entre la URSS y China, lo que en última instancia terminaría por beneficiarle en el esquema de la confrontación bipolar. Así, Washington favoreció y respaldó las reformas iniciadas por Deng Xiaoping a fines de los años setenta. Éstas, de acuerdo con Kobayashi, Baobo, y Sano (1999), partían del reconocimiento de que China se encontraba económicamente devastada tras la revolución cultural y necesitaba ser reconstruida. La estrategia de Deng, la "economía socialista de mercado", consistía en mantener el sistema comunista, pero con una política de puertas abiertas a través de la introducción de capital y tecnología extranjeros para detonar el crecimiento del país y tratar de elevar el ingreso medio de los trabajadores. Para ello era indispensable levantar flujos masivos de capital foráneo.

Esto detonó un crecimiento económico tal que para 1998, el producto per cápita chino era 14 veces mayor que en 1980 y 20 años después, en 2018, se había multiplicado incluso 10 veces más que en 1998. La población china viviendo por debajo de la línea de la pobreza en 1980 era 88% del total. Para el 2017, ese porcentaje había bajado a únicamente el 6% (Zhou y Xiao, 2018).

Ahora bien, ese capital extranjero fluyó mucho menos de las economías industrializadas, y mucho más de economías vecinas a China tales como Hong Kong y Taiwán. Para 1994, la inversión procedente de EEUU era únicamente del 7% del total de Inversión Extranjera Directa (IED) en China. Veinte años después, la IED en China había crecido cinco veces, pero de este total, solo 2.3% procedía de EEUU y únicamente 13% procedía de economías industrializadas combinadas. En cambio, el otro 87% procedía de otros países (Federal Reserve Bank of Minneapolis, 2016).

El apareamiento económico entre China y EEUU se va a gestar esencialmente en el plano del intercambio comercial. Según el censo estadounidense, las exportaciones chinas hacia EEUU, que en 1985 sumaban poco más de 3,800 millones de dólares, hacia 2018 ascendieron a más de 539 mil millones de dólares. Esto representa una quinta parte de todo lo que EEUU importa en la actualidad. Aunque menos, el comercio también creció enormemente en la otra dirección. De unos 3,800 millones de dólares en 1985, EEUU ha pasado a exportar a China más de 125 mil millones de dólares. Esto no solo representa un intercambio entre dos países, sino una verdadera sociedad comercial con todo lo que ello implica.

Pero aún considerando esa sociedad comercial, el asunto se complejiza más si no solo pensamos en el tráfico de materias primas o productos terminados. De lo que estamos hablando, sobre todo en las últimas décadas, es de la construcción y afianzamiento de importantísimas cadenas de abasto, muchas de las cuales no solo involucran a EEUU y a

China sino a otros países, pero que en el caso de esas dos superpotencias contribuyen considerablemente al apareamiento económico que mencionamos. Sectores como el de la electrónica, maquinaria avanzada y partes industriales dependen del libre tránsito de componentes y materiales diversos. De hecho, ahora mismo, a raíz de los aranceles impuestos por EEUU a varios de los sectores mencionados, muchas empresas chinas se están viendo obligadas a encontrar formas para mantener vivas esas cadenas de abasto. De acuerdo con Guilford y Kopf (2019), el gobierno de Vietnam descubrió recientemente una sustancial cantidad de bienes chinos, desde acero hasta productos agrícolas, etiquetados ilegalmente como "hechos en Vietnam". Otro tipo de tácticas que sí son legales, sin embargo, incluyen la triangulación de las exportaciones chinas hacia EEUU a través de enviar las partes a sitios como Taiwán y Vietnam, y ensamblarlas posteriormente como productos manufacturados en esos países (Guilford y Kopf 2019).

Por si fuera poco, a lo largo de todos estos años, China se convirtió en el mayor acreedor de la deuda estadounidense. Para mayo del 2019, la deuda de los EEUU a China ascendía a 1.11 billones de dólares, es decir, el 27% de bonos del Tesoro y otros instrumentos que poseen otros países (Departamento del Tesoro de los EEUU, 2019). El segundo acreedor de EEUU es Japón. Si bien se ha dicho que este factor podría ser utilizado por China en un momento de desesperación en la guerra comercial, la realidad es que estas circunstancias hacen que ambas economías se vuelvan interdependientes. Sobra decir por qué un deudor desarrolla dependencia de su acreedor, pero al mismo tiempo, no está en el interés de un acreedor que su deudor tenga problemas económicos.

Es indispensable, entonces, comprender lo que esto implica: (a) la vinculación o asociación económica es una realidad material que genera intereses no solo entre los propios gobiernos, sino también entre actores no estatales que no necesariamente se encuentran apareados con los intereses de sus estados sede, y por tanto, (b) que la decisión estratégica de activar instrumentos diversos, desde económicos hasta militares, para librar una guerra que tenga la meta última de debilitar a la contraparte, supone la puesta en marcha de una serie de medidas muy concretas para disminuir la interdependencia económica y financiera, lo que solo se conseguiría reorientando inversiones, comercio y cadenas de abastos hacia afuera de China y con ello, redireccionar los intereses de todos esos actores no estatales que hoy se ven perjudicados con las disputas geopolíticas.

Por tanto, debido a todo el costo que implicaba, tuvo que pasar mucho tiempo, y una confluencia de circunstancias, incluido el ascenso de Trump a la presidencia, antes de que Washington decidiera activar la espiral de la desvinculación económica.

Acá sin embargo, es importante entender que cuando un personaje con las características específicas del actual presidente estadounidense impone aranceles, argumentando que quiere reducir el déficit comercial que EEUU tiene con China o erradicar el comercio injusto, no está necesariamente pensando en geopolítica, sino en política (y no es lo mismo). En la mente de Trump están temas como "America First" (Estados Unidos Primero), mostrarse como un presidente que cumple con su base y sus compromisos de campaña, que "cuida" a los trabajadores estadounidenses. Trump quiere reelegirse y pasar a la historia como el presidente que combatió todos los "tratos injustos" de que la superpotencia ha sido sujeta por parte de otros países que se han "aprovechado" de la "ineficacia" de mandatarios previos, republicanos y demócratas por igual. Lo que sucede es

que, en el caso concreto de China, resulta que la visión de Trump hoy tiene varios puntos de coincidencia con otros actores en Washington quienes sí están pensando en cómo reorientar la estrategia de largo plazo de la máxima superpotencia para contener la expansión de China.

Es por ello que vale la pena distinguir entre el corto y el largo plazo. En el corto plazo hay elecciones en EEUU, hay una campaña de Trump, y hay la necesidad de mostrar eficacia inmediata en cuanto a las estrategias negociadoras del presidente. De ahí que éste pueda lanzar desde Twitter líneas como esta: "Se ordena por este medio a las compañías estadounidenses comenzar a buscar alternativas fuera de China", provocando pánico en las cadenas de abasto arriba señaladas. A ese tuit, únicamente siguió el anuncio de incrementos arancelarios. Sin embargo, al momento de este escrito, muchas personas temen que la Casa Blanca pueda invocar las facultades bajo el Acta de 1977 sobre Poderes Económicos de Emergencia Internacional para obligar a las compañías a salir de China (Stratfor, 2019).

No obstante, más allá de los tuits o de las cuestiones de política interna, las cadenas de abasto establecidas a lo largo de estas décadas no pueden ser deshechas en unos cuantos meses. En todo caso estamos hablando de procesos de años. Por tanto, hay quienes piensan que solo se trata de estrategias de negociación y no de medidas estructurales para desvincular a las economías.

Pero ese es precisamente el punto. Una cosa es lo que pase por la mente de Trump, y otra muy distinta es la dinámica espiral de un conflicto de fondo que no solo está compuesto por la arista comercial.

3. De la guerra contra el terrorismo al Instituto Hudson: las distintas líneas de enfrentamiento EEUU-China

Como se indicaba arriba, a raíz de los atentados del 11 de septiembre del 2001, la prioridad de seguridad de Washington durante la gestión de Bush y la de Obama fue la lucha contra el terrorismo. Ya sea por un error en la estimación de la peligrosidad comparada de organizaciones terroristas en contraste con la amenaza que representaban las superpotencias rivales de EEUU, o quizás, por la misma evolución de las relaciones entre Washington y esas otras superpotencias, o bien, debido a una estrategia calculada, durante estas décadas la Casa Blanca se concentró mucho más en su enfrentamiento con dichas organizaciones terroristas y menos en su enfrentamiento con otros estados.

Esto no significa que a lo largo de esos años no había preocupación por lo que ocurría con Rusia o China, sino que el enfoque primario de Washington del 2001 al 2017 estuvo en el combate al terrorismo.

Como lo señalamos arriba, la Estrategia de Seguridad Nacional del 2017 y la Estrategia de Defensa Nacional en 2018 fueron los documentos que marcan el cambio.

Más aún, como nos explica Schake (2018), dada su capacidad económica, militar y tecnológica, y dada su proyección hacia el largo plazo, China es percibida como una mayor amenaza que Rusia. De ahí que el viraje en la estrategia de Seguridad Nacional estadounidense ponga especial énfasis en Beijing. De hecho, apenas unos días antes de esta publicación (septiembre, 2019), el Equipo de Transición del Ejército de EEUU recomendó a las fuerzas armadas cambiar su foco primario desde Rusia y Europa hacia China y la

región Asia-Pacífico. Esto se asomaba con fuerza ya desde el discurso del vicepresidente Mike Pence ante el Instituto Hudson (2018).

Algunos de los aspectos centrales de ese discurso son los siguientes: (1) La concepción de que China está empleando un esfuerzo dirigido desde el gobierno que involucra a toda la administración pública, agencias y ministerios, para conseguir sus intereses de influencia global y específicamente profundizar su influencia en los EEUU. Esta serie de acciones conducidas desde el estado, incluye instrumentos políticos, económicos y militares, además de propaganda y una guerra informativa; (b) La concepción de que este esfuerzo proactivo por parte de Beijing para ejercer influencia e interferir en la política interna estadounidense está siendo desplegado como nunca antes en el pasado y de manera cada vez más clara; (c) La concepción de que la búsqueda de influencia china no se limita a su propia región—Asia—sino que pretende expandirse hacia otros continentes; (d) Una visión negativa del déficit comercial de EEUU a favor de China, así como de iniciativas económicas como el programa *Made In China 2025*, y de infraestructura global como la *Iniciativa Cinturón y Ruta* (BRI); (e) La concepción de que China utiliza el endeudamiento de otros países, el comercio, la inversión y los lazos económicos que tiene para avanzar sus propios intereses, lo que incluye el robo de tecnología, investigación, desarrollo e innovación o la presión en contra de diversos gobiernos, incluidos algunos latinoamericanos, para alinearse con la visión geopolítica y estratégica de Beijing; (e) La idea del riesgo que representa el que China esté aumentando su gasto militar como lo ha hecho en los últimos años, así como el expansionismo en sus mares colindantes; (f) Concretamente, la acusación directa de que Beijing impide las operaciones de "libertad de navegación" y "acosa" a los navíos estadounidenses en "aguas internacionales"; (g) La concepción de China como un estado autoritario, espía, violatorio de los derechos humanos, opresor de las minorías y de su propio pueblo, y (h) De todo lo anterior se sigue la necesidad que tiene Washington de tomar pasos firmes para enfrentar cada una de esas estrategias de Beijing.

Esta visión, por cierto, como ya lo dijimos, no necesariamente retrata del todo propiamente a Trump, sino que ofrece una imagen procedente de otros círculos duros en Washington que mantienen esta serie de argumentos desde tiempo antes de la actual administración y que han conseguido ejercer una notable influencia sobre el presidente.

De su parte, la agencia oficial de noticias china, Xinhua (2018), respondió en su sitio web a este discurso con un texto titulado "Las cinco falacias del discurso de Pence sobre China". Para esta agencia, en el discurso de Pence, se puede apreciar una especie de "sinofobia" que refleja concepciones erradas acerca de Beijing y sus metas. Estas cinco falacias son las siguientes: (1) Estados Unidos no fue quien "reconstruyó China" como lo afirma el vicepresidente Pence; el crecimiento y desarrollo de ese país son producto de su propio trabajo; (2) no hay tal "expansionismo chino", sino una "defensa justa" de sus intereses centrales y "legítimos derechos". En cambio, es EEUU quien se mantiene retando a Beijing en Taiwán y en Mar del Sur de China, así como en otras cuestiones de la región; (3) para Xinhua, Pence solo acusa a China de prácticas comerciales injustas, ignorando el beneficio mutuo del intercambio comercial bilateral. Es verdad que China ha crecido gracias al comercio, pero dicho comercio ha traído a las empresas estadounidenses acceso a "un mercado masivo", a los consumidores estadounidenses "productos de calidad a bajo precio", y a la economía estadounidense "incentivos para mejorar"; (4) de acuerdo con el texto, Pence parece ignorar las profundas reformas y apertura política y económica de

China, un largo proceso que lleva años, y (5) por último, para Xinhua, la influencia que, según Pence, China busca proyectar, así como su injerencia en procesos electorales estadounidenses, son meras ilusiones no respaldadas por evidencia.

En resumen, ya sea por una serie de percepciones mutuas que se han venido distorsionando a lo largo de los años, o por concepciones equivocadas acerca de quién es y qué busca en el fondo cada uno de los rivales, o bien, por factores estructurales del sistema internacional y la natural tendencia al choque ocasionada por el crecimiento de un poder emergente frente al declive relativo de un poder existente, lo que tenemos ante nosotros parece ser un enfrentamiento de largo plazo, probablemente distinto a como ha ocurrido en otros casos históricos, el cual ha activado dinámicas conflictivas propias que bien pueden rebasar las voluntades de individuos o actores políticos específicos, y el cual puede ser, sin embargo, contenido gracias a que no está solo caracterizado por el conflicto sino que incluye espacios para cooperación. Esto último, como dijimos, es un proceso en constante evolución, pero que estará determinado por la combinación de lo que resulte de las diversas áreas de enfrentamiento.

Sin buscar profundizar en dichas áreas de enfrentamiento, las mencionamos a continuación con el objetivo de aportar una mirada panorámica y comprender la dimensión tecnológica a partir de su inserción en toda esta dinámica:

a. **La expansión china en sus mares colindantes.** Desde hace algunos años, Beijing viene estableciendo posiciones en zonas disputadas por distintos países de la región, lo que incluye islas, islotes, rocas e islas artificiales. Además de perseguir objetivos de explotación económica de estas zonas disputadas, China ha estado ubicando personal militar y armamento, lo que representa un abierto reto a los reclamos de otros países de la región. Para Beijing, como vimos arriba, estas acciones no son otra cosa que el ejercicio de su legítimo derecho sobre espacios geográficos que son de su propiedad. Naturalmente, sus vecinos piensan diferente. Pero al margen de ello, en los últimos años hemos presenciado una creciente determinación de Washington para hacer prevalecer su estatus como la potencia dominante en el Pacífico, estatus que mantiene desde la Segunda Guerra Mundial, así como para defender a sus aliados regionales. Por ello, para la Casa Blanca ha sido esencial transmitir el mensaje de que hará cuanto sea necesario para desafiar el expansionismo chino, lo que se ha traducido, entre otras medidas, en expediciones de "libertad de navegación" por parte de buques militares estadounidenses, así como operaciones aéreas en la región. En más de una ocasión, navíos o aviones estadounidenses han estado cerca de colisionar con buques o aviones chinos, situación que pudiera derivar en incidentes delicados. Adicionalmente, en tiempos más recientes estamos ya también viendo ejercicios navales conjuntos entre la Marina de EEUU y otros países de la región en el Mar del Sur de China, en respuesta a ejercicios navales que China ha estado también llevando a cabo.

b. **Taiwán.** Este tema, particularmente sensible para Beijing, ha estado en la agenda cada vez más en los últimos años. Esto obedece a una aparente decisión por parte de la administración Trump de emplear la cuestión Taiwán como instrumento de presión en el medio de toda la conflictiva que sostiene con Beijing. Desde el inicio de su gestión, Trump ha intentado mostrar signos de cercanía política y militar con

la isla, la cual para China es una provincia en rebelión. Entre otras acciones, recientemente la Casa Blanca aprobó ventas por 2,200 millones de dólares a Taiwán en tanques, misiles y equipo militar. Hace pocas semanas el gobierno estadounidense anunció que procedería con ventas de aviones de combate F16 a Taipéi en lo que representa una de las mayores transacciones de esta índole entre EEUU y Taiwán. La respuesta de Beijing no se ha dejado esperar. China ha declarado que sancionaría a cualquier empresa vinculada con las ventas de tanques, aviones o equipo militar a la isla.

c. **Corea del Norte.** Tras un 2017 de escaladas retóricas, ensayos nucleares, pruebas con misiles de mediano y largo alcance, además de ejercicios militares, en 2018 atestiguamos un viraje caracterizado por la distensión y las conversaciones. De hecho, Trump ha apostado una buena parte de su capital político en el progreso de las negociaciones con Pyongyang. Sin embargo, en este tema, el factor China resulta crucial pues Beijing es el principal sostén y aliado del régimen norcoreano. Por más sanciones o elementos que se ha buscado emplear para presionar a Pyongyang, éstos solo cuentan con una eficacia limitada cuando no se consigue la plena colaboración de China en su implementación. Al mismo tiempo, la supervivencia del régimen norcoreano sigue formando parte del interés de China. Por tanto, cualquier iniciativa que excluya a Beijing de la mesa, o bien, que rompa los equilibrios que China estima adecuados, será vetada u obstaculizada por Beijing. De igual modo, si la dinámica conflictiva entre Washington y China sigue escalando en los otros rubros que se mencionan, es posible que Xi Jinping emplee a este como un factor adicional para ejercer su propia presión sobre Trump y deje de cooperar en donde es indispensable. Por último, ya en 2017 pudimos observar la reacción china ante la instalación del sistema estadounidense de Defensa Aérea de Alta Altitud Terminal (THAAD) en Corea del Sur. El enojo de Beijing se hizo sentir en temas comerciales con Seúl, y aunque esa disputa ha sido relativamente desescalada, China permanecerá con la mira puesta en el incremento de actividad militar y el despliegue de armamento ofensivo o defensivo en la península.

d. **Carrera armamentista y despliegues de misiles.** De manera separada al tema previo, está la carrera armamentista y la intención de EEUU de desplegar misiles de rango intermedio en zonas geográficas que pudieran impactar a China. Además de la preocupación que provoca en Washington los monumentales esfuerzos de los últimos años para robustecer las capacidades del ejército y la marina chinos, EEUU nunca logró que Beijing se comprometiera a formar parte del Tratado sobre Fuerzas Nucleares de Rango Intermedio (INF)—convenio firmado en 1987 entre Reagan y Gorbachov—o que firmase un nuevo tratado que le incluyera. De modo que la creciente rivalidad de Washington con Beijing parece haber sido uno de los factores principales que orillaron a la Casa Blanca a decidir abandonar aquél pacto que tenía con Rusia. Ahora la cuestión será ver si es que las superpotencias lograsen llegar a un acuerdo para primero, garantizar la supervivencia del Nuevo START (Strategic Arms Reduction Treaty)—el último tratado que persiste para regular la posesión de armamento nuclear entre los grandes poderes—y segundo, incluir la firma de Beijing en ese tratado del que actualmente no forma parte. Sin embargo, dada la dinámica conflictiva y la desconfianza que se está produciendo, hoy no hay

demasiadas razones para el optimismo en este tema, lo que detonaría una carrera nuclear de dimensiones imprevisibles. Más aún, las recientes pruebas con misiles de tierra efectuadas por EEUU tras su salida del INF provocaron ira en Beijing, quien acusó a Washington de estar penetrando en una "mentalidad de Guerra Fría". Adicionalmente, el anuncio de Washington de que, tras su salida del INF, desplegará misiles intermedios convencionales en la zona del Pacífico Occidental, los cuales incluyen en su rango a China como objetivo potencial, no ha hecho sino inflamar más las llamas de la desconfianza a que nos referimos.

e. Cooperación Rusia-China. A pesar de que, tanto en el pasado, como en el presente y, por supuesto, en el largo plazo, sus intereses han tendido y tenderán a competir e incluso a chocar, ya desde hace algunos años estamos viendo un incremento en la cooperación entre Moscú y Beijing. Esto se ha observado desde cuestiones como la adopción de posiciones diplomáticas conjuntas en temas diversos y votos comunes en el Consejo de Seguridad de Naciones Unidas, o el apoyo ruso a *la Iniciativa Cinturón y Ruta* (Belt and Road Initiative o BRI) y la Nueva Ruta Marítima de la Seda—lo que contempla la colaboración con Beijing para temas de infraestructura, logística e incluso el trabajo conjunto para la Ruta Norte en el Ártico—hasta la cooperación militar como ejercicios militares conjuntos y ejercicios navales conjuntos. Hace unos meses tuvo lugar el primer patrullaje aéreo conjunto de largo alcance entre la fuerza aérea china y la rusa sobre islas disputadas entre Corea del Sur y Japón. Los sucesos recientes tanto en la esfera geopolítica Rusia-Washington como en la dinámica Washington-Beijing seguirán propiciando espacios para la cooperación entre China y Rusia, lo que, sin duda, contribuirá a inflamar más aún las llamas de la desconfianza entre Washington y Beijing.

f. La competencia por la influencia económica y el poder blando. En este rubro vale la pena resaltar no solo la decisión china de incrementar su esfera de influencia económica y política, sino cómo es que estas metas son percibidas por Washington y las acciones tomadas desde la Casa Blanca para contener lo que es visto por ésta como un expansionismo peligroso. Como ya dijimos, China ha venido desarrollando desde hace unos años un proyecto denominado *Iniciativa Cinturón y Ruta* (BRI). Beijing está buscando impulsar el enlace por tierra y por mar, de rutas comerciales que conecten Europa con Asia para revivir la antigua "ruta de la seda" que vinculaba a esas tierras lejanas. El proyecto maestro de Xi Jinping consiste en el desarrollo de infraestructura, puertos, caminos y vías marítimas, e incluye a decenas de países. Para EEUU, se trata de un mecanismo mediante el cual Beijing consigue incrementar la dependencia económica, comercial y financiera de diversos países, y ha protestado cuando encuentra que los proyectos de China tocan a sus aliados. Un caso reciente es el de Italia, pero otro muy interesante es el de Israel. Con todo lo cercana que es la administración Trump al gobierno de Netanyahu, Washington ha pintado su línea y ha indicado que, si Tel Aviv continúa sus proyectos de inversión con China, esto dañaría las relaciones entre EEUU e Israel. A pesar de esa presión, e incluso a pesar de la advertencia de que la inversión china en infraestructura en una zona de seguridad muy sensible podría hacer a Israel correr riesgos de información crítica, Tel Aviv está procediendo con este tipo de proyectos provocando irritación en la Casa Blanca.

América Latina es, sin duda, uno de los casos más sensibles para Washington. La expansión de las inversiones chinas en nuestro continente es frecuentemente percibida entre los sectores más duros en Estados Unidos como abiertos intentos para incrementar la influencia china en una órbita que Washington considera de influencia exclusiva: el hemisferio occidental. Esto es parte de lo que queda claro en el discurso de Pence, arriba referido.

g. Ciberguerra y guerra informativa. Más allá de considerar la carrera tecnológica provocada por la competencia entre las superpotencias, es importante comprender que desde hace años este espacio se vuelve un escenario ideal para rivalizar o golpear al adversario dado que esto puede llevarse de manera relativamente obscura, sin la necesidad de responsabilizarse de cierto ataque. Siempre hay espacio para negar la autoría. Es más, la parte atacada puede decidir hasta qué punto atribuye o no atribuye la responsabilidad de esos ataques al rival.

Considere este caso: en 2013, una firma de seguridad internacional llamada Mandiant, detallaba las potenciales ligas del ejército chino con cientos de ciberataques efectuados en contra de diversas agencias, empresas e instituciones estadounidenses desde la Coca Cola hasta Lockheed Martin. Entre las víctimas había compañías dedicadas a tecnología, satélites o comunicaciones, así como armamento, plantas químicas, hospitales y universidades. No se trataba exclusivamente de robo de información o espionaje, sino de la capacidad de manipular e intervenir en el manejo de infraestructura crítica dentro de Estados Unidos. Toda esta investigación apuntaba a una misma ubicación en Shanghái: el edificio de la unidad 61398 del ejército chino. Desde ese sitio operaba la denominada "Comment Crew", o "Grupo Shanghái", el responsable del 90% de estos ciberataques. Sin embargo, debido a que Beijing no reconocía responsabilidad alguna en estos eventos, la Casa Blanca había elegido mantener la cautela en sus acusaciones para evitar dos riesgos: (a) que se sacara a la luz los ciberataques en los que el propio gobierno estadounidense había sido implicado anteriormente, y (b) complicar las relaciones con China en un momento sumamente delicado en materia geopolítica. No obstante, los ciberataques chinos continuaron y la administración Obama se vio forzada a hacer algo al respecto. En mayo de ese año, se eligió al Pentágono para que hiciese la denuncia. Beijing, por supuesto, negó su involucramiento en el tema y se dijo, una vez más, la víctima. Pero la presión sobre Obama siguió aumentando y no le quedó alternativa que hacer el reclamo personalmente. Fue entonces cuando Snowden apareció en la escena. Entre sus muchas revelaciones, el exempleado de la CIA—desde Hong Kong, territorio chino—relataba que Washington hacía contra Beijing exactamente lo mismo que aquello de lo que se decía víctima. A partir de entonces el foco se trasladaba hacia las actividades de espionaje conducidas por agencias estadounidenses, muchas de las que eran violatorias de la privacidad de ciudadanos y funcionarios de diversos países, amigos y enemigos por igual.

Con todo, la esfera digital ofrece, podríamos decir, un canal de salida de costo relativamente bajo para librar una guerra de desgaste y de baja intensidad. Se puede

golpear al contrincante sin la necesidad de usar bombas, aviones, buques, sin provocar muertes y, sobre todo, sin detonar una espiral de violencia que pudiera derivar en un conflicto armado de proporciones mayúsculas.

Dicho lo anterior, estamos ante una importante escalada tanto de ciberataques como de la guerra informativa. La enorme dependencia de la tecnología vuelve a empresas, organizaciones y agencias públicas altamente vulnerables ante este tipo de ataques. Adicionalmente, en los últimos años hemos visto cómo determinados actores asociados a los ejércitos, agencias de inteligencia y gobiernos de las superpotencias, emplean el internet y las redes sociales para buscar influir en cuestiones políticas o en procesos electorales. En este último punto, conocemos las acusaciones de EEUU en contra de China y Rusia—lo que representa la decisión contundente de atribuir formalmente la responsabilidad de estos hechos a las superpotencias rivales y, por tanto, la consecuente necesidad de responder mediante sanciones o mediante medidas simétricas. Sin embargo, es importante también considerar que Washington lleva años preparándose y trabajando en este rubro, no solo para defenderse, sino también para atacar. Es con esto en mente que hay que revisar nuestra posterior sección acerca de la dimensión tecnológica. Es decir, más allá de una “competencia” entre dos rivales que buscan ganar espacio de mercado e influencia, se trata de superpotencias que emplean la esfera tecnológica como zona de choque.

Parte II: la dimensión tecnológica del enfrentamiento EEUU-China

1. El ascenso de China como líder en tecnología.

La dimensión tecnológica del conflicto entre China y EEUU tiene implicaciones multidimensionales, que van mucho más allá del intercambio económico y la obtención de rentas. En su lucha por dominar cada terreno, la tecnología y sus posibles usos adquieren una importancia sin precedentes. Aspectos relacionados con seguridad nacional, privacidad, propiedad intelectual, derechos humanos, ética e influencia política, hacen eco en las discusiones sobre el uso de tecnologías y equipos de origen chino.

El surgimiento de China como potencia en tecnologías de la información y la comunicación (TICs), principalmente representada por el ascenso de Huawei y su posición en el mapa mundial de las telecomunicaciones, ha generado temores, acusaciones y bloqueos en EEUU, que ha argumentado que la nueva posición china se debe a presiones sobre ciertas democracias occidentales y al robo de tecnología. También ha dicho que los usos de esas tecnologías por parte de las empresas y el gobierno chino resultan cuestionables, poniendo en riesgo la seguridad nacional e, incluso, la paz global (The Economist, 2019).

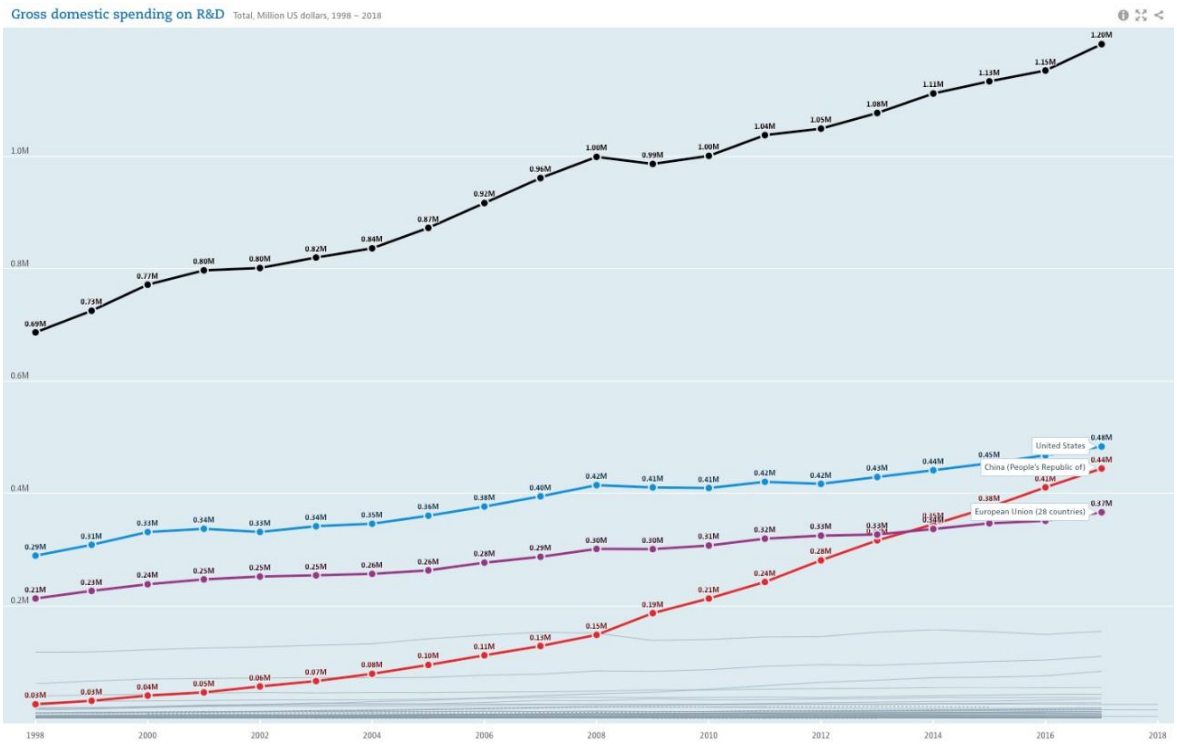
En el presente apartado analizamos brevemente el camino que ha seguido China para convertirse en esa potencia tecnológica, particularmente durante las últimas dos décadas.

Aunque la llamada "carrera espacial" –iniciada en 1957 con el lanzamiento del Sputnik, el primer satélite artificial– no tenga las mismas implicaciones hoy que hace 60 años, la exploración espacial continúa siendo un claro referente de poderío científico y tecnológico. Es por ello que China ha ingresado, tardíamente, pero con audacia a esta carrera y ha ofrecido demostraciones contundentes de su ambición en la materia. Prueba de ello fue la misión de exploración lunar *Chang'e 4* que el 3 de enero de 2019 logró alunizar en el cráter Von Kármán, ubicado en el lugar más lejano de la luna, fuera del alcance de la vista de los controladores en tierra. Se trata de un punto en el que la única forma de colectar, enviar y recibir datos e información es a través de satélites de retransmisión[1]. Estamos ante una misión que exige un despliegue tecnológico monumental para llegar a un lugar al que nadie, hasta ahora, había podido. Por supuesto, se trata también de una demostración del poderío económico chino.

La materialización de proyectos como la misión *Chang'e 4* es un claro ejemplo de lo que China está dispuesta a hacer para mostrarse al mundo como una superpotencia tecnológica. Esto no se puede lograr sin grandes sumas de inversión, y por eso no sorprende que China haya incrementado en los últimos 17 años más de diez veces su inversión en investigación y desarrollo. Esta pasó de alrededor de 40 mil millones de dólares en el año 2000, a más de 444 mil millones en el 2017, muy cercanos a los 483 mil millones que destina EEUU para ese propósito[2], y por encima de la Unión Europea en su conjunto (OCDE, 2019).

[1] Los satélites en órbita no son capaces de transmitir información a las estaciones en Tierra, si el satélite no tiene una clara línea de visión a dichas estaciones. Los satélites de retransmisión sirven para ese propósito. NASA. What is a relay satellite? Disponible en: https://www.nasa.gov/directorates/heo/scan/communications/outreach/funfacts/txt_relay_satellite.html

[2] Estos montos se refieren a la inversión total en investigación y desarrollo en un país, llevada a cabo por todas las empresas residentes, institutos de investigación, universidades, laboratorios de investigación, etc.



Gráfica 1.0: Comparación entre la inversión en tecnología de China (rojo) con Estados Unidos (azul) y los 28 países de la UE combinados (violeta). Fuente OCDE (2019).

Estos incrementos de inversión se han visto rápidamente reflejados en diversos indicadores que demuestran que China poco a poco va tomando una posición de liderazgo en ciencia y tecnología. Por ejemplo, un estudio publicado por Elsevier para la agencia de noticias Nikkei en enero de 2019, concluyó que China domina el ranking global de los artículos de investigación más citados en las 30 áreas tecnológicas de mayor interés, al contar con la contribución más grande en 23 de esas áreas, mientras que EEUU mantiene el primer lugar tan solo en las siete restantes. Resalta la particularidad de que China ha enfocado su investigación y desarrollo en áreas con potencial comercial, como la electrónica y los vehículos eléctricos (Okoshi, Nikkei Asian Review, 2019). Aunque la calidad de la investigación ha sido criticada, los indicadores muestran que ésta ha mejorado con el paso de los años y cada vez genera un mayor impacto entre los investigadores a nivel global.

Estos avances han sido impulsados a través de diversas políticas del gobierno chino, entre las que conviene destacar dos para efectos del presente análisis: (i) la creación de un grupo de universidades de élite conocidas como la *Liga C9*, y (ii) el plan *Made in China 2025*.

La *Liga C9* de universidades chinas se trata de una política iniciada por el gobierno desde 1998. Posteriormente, y como parte de los esfuerzos por aumentar la investigación y desarrollo, fue consolidada mediante el “Programa de Mediano y Largo plazo para la Reforma a la Educación y el Desarrollo” lanzado en 2010. Esta iniciativa consiste en la selección del gobierno chino de ciertas universidades—originalmente 9 que se

incrementaron a 39 en 2011—para invertir en ellas a fin de potenciar el desarrollo de disciplinas técnicas y científicas. Se estima que las nueve universidades de la inicial *Liga C9* han recibido alrededor del 10 por ciento del gasto público en investigación y desarrollo, lo que ha contribuido a que una quinta parte de artículos publicados a nivel nacional provenga de estas universidades, y que el 30 por ciento del total de citas sea a autores de dichas publicaciones (Luo, 2013).

Por otra parte, el plan *Made in China 2025* fue lanzado por el Primer Ministro Keqiang en 2015 con el objetivo de transformar al país en una potencia tecnológica mediante la implementación de "políticas favorables a la reestructuración de la industria tradicional manufacturera, con especial énfasis en innovación, propiedad intelectual y desarrollo sostenible" (Gómez, 2016). Esta política abarca 10 sectores clave, entre los que se encuentran equipamiento eléctrico, equipamiento aeroespacial, ahorro energético, vehículos de nuevas energías y, por supuesto, tecnologías de la información.

Made in China 2025 pretende, entre otros objetivos, incrementar el contenido local de componentes básicos y materiales a un 40 por ciento para el año 2020 y a 70 por ciento para el 2025. La finalidad es obtener un mercado autosuficiente para las empresas locales, de manera que les permita competir por mayores participaciones de mercado a nivel global (Cyrril, 2018).

Como era de esperarse, el plan levantó sospechas de otros países respecto a los extensos apoyos estatales que se estarían otorgando, ya sea en forma de subsidios o financiamiento, a empresas públicas o privadas. El gobierno estadounidense considera esto como competencia desleal y por eso *Made In China 2025* ha sido un factor fundamental en la guerra comercial entre ambos países. Algunos autores han señalado que este plan se convirtió en el objetivo central del Reporte de la Oficina del Representante de Comercio de los Estados Unidos (USTR por sus siglas en inglés), conforme a la sección 301 de la Ley de Comercio de 1974 (Chen, 2019; Sheehan, 2018), al que nos referiremos posteriormente, y que fue el detonante de dicha guerra comercial.

Bajo el contexto descrito, la expansión de la industria tecnológica china a nivel global es hoy una realidad que ha adquirido proporciones mucho mayores a las anticipadas por EEUU y sus aliados. Ante las restricciones impuestas por parte del gobierno estadounidense en 2018 a una compañía de origen chino—ZTE—el presidente Xi Jinping respondió exponiendo una amplia visión para consolidar a China como una superpotencia tecnológica. No sólo eso: también se busca convertir a China en una "ciber-superpotencia" (Heatley, 2018) que lidere el mundo en cuanto a inteligencia artificial (IA), computación cuántica, semiconductores, biología sintética, energía renovable y la llegada de la generación 5G de redes móviles (The Economist, 2018).

Con esta visión, China ha creado nuevas instituciones como el "Grupo Central de Estudios Teóricos", dependiente de la Administración China del Ciberespacio (ACC). Este grupo publicó en 2017 un artículo en el que se describen los principales elementos de la visión estratégica de Xi Jinping en política del ciberespacio: (i) manejo del contenido de internet y creación de una "energía positiva" en línea; (ii) garantizar la ciberseguridad, incluyendo la protección de información sobre infraestructura critica; (iii) desarrollar una base tecnológica doméstica e independiente para el *hardware y software* que afiance el internet

en China, y (iv) incrementar el rol de China en la construcción, gobernanza y operación del internet a nivel global (Kania *et. al.*, 2017).

De esta forma, China ha venido construyendo una clara ruta para pasar de ser una economía que dependía ampliamente de tecnologías extranjeras a producirlas y, en muchos casos, ha conseguido posicionarse como líder en diversos mercados internacionales. Esto ha generado cuestionamientos sobre cuatro temas importantes: (i) la forma en la que China ha logrado este ascenso; (ii) preocupaciones sobre el poder que China puede ejercer sobre otras naciones a través de las tecnologías; (iii) potenciales represalias motivadas por cuestiones comerciales; y (iv) implicaciones de seguridad nacional, tal como se describe en los siguiente apartados.

2. La disputa tecnológica: Huawei y las redes 5G

Huawei es el ícono del ascenso global de China en tecnología, tanto por su veloz crecimiento –la empresa tiene poco más de 30 años– como por los mercados que hoy lidera. Basta decir que, junto con la finlandesa Nokia y la sueca Ericsson, se ha convertido en uno de los más grandes proveedores mundiales del kit necesario para el despliegue de redes de telefonía móvil (The Economist, 2019), así como uno de los líderes globales en el desarrollo de tecnologías de siguiente generación, a grado tal que podría dominar el despliegue mundial de redes 5G.

Huawei opera en más de 170 países, al 2018 contaba con alrededor de 180,000 empleados a nivel internacional y sus ingresos sumaban 40,000 millones de dólares (Tao *et. al*., 2018), cifras por sí mismas impresionantes, pero que sorprenden más si consideramos que hace apenas una década la empresa todavía contaba con poca presencia fuera de su país de origen.

La expansión de Huawei se ha dado en tres etapas. La primera fue a finales de los años 80 del siglo pasado, mediante el dominio del mercado nacional. La segunda etapa va de 1993 al 2000, cuando se dieron reestructuras de la compañía ante la apertura comercial, así como alianzas comerciales con empresas occidentales para el aprendizaje. La tercera etapa inicia a partir del año 2000 y está marcada por la acelerada internacionalización de la compañía, impulsada en buena medida por el incremento en la demanda mundial de teléfonos móviles. Desde 2006, más del 65 por ciento de los ingresos de la compañía provienen de los mercados internacionales (Micheli y Carrillo, 2016).

El posicionamiento de Huawei en el mapa mundial de las telecomunicaciones, incluso desde una etapa temprana, ha sido objeto de controversia y diversos cuestionamientos, originados principalmente en EEUU. La naturaleza de los cuestionamientos ha sido sumamente amplia; sin embargo, se pueden englobar en 4 aspectos fundamentales: (i) apoyo financiero del gobierno chino; (ii) disputas sobre derechos de propiedad intelectual; (iii) estrechos vínculos de la empresa con el ejército chino; y (iv) amenazas a la seguridad nacional de EEUU (Tao, *et al.*, 2018).

En cuanto a los apoyos gubernamentales, por ejemplo, Cisco ha asegurado que la empresa recibe 30,000 millones de dólares anuales del gobierno Chino. Huawei ha negado esto en varias ocasiones, al asegurar que se trata de una empresa privada que es “100 por ciento propiedad de los trabajadores” porque 80,000 de ellos son accionistas de la compañía. Asegura también que su fundador, Ren Zhengfei únicamente conserva el 1.4 por ciento de

las acciones (Tao, *et al.*, 2018). Empero, hay que señalar que la estructura accionaria de la compañía es desconocida (Weber, 2018).

Las afirmaciones de apoyos gubernamentales han sido además alimentadas por la política china de "Campeones Nacionales", que se enmarca en los planes del gobierno para extender sus objetivos estratégicos a nivel global. Un hecho que desata polémica en Occidente es la existencia de un "Comité del Partido Comunista" en la empresa, que ha sido defendido bajo la justificación de la necesaria moralidad y responsabilidad social entre los líderes de la compañía. A pesar de la defensa que la compañía hace de este comité, es difícil dejar de considerar este elemento dentro del panorama amplio que hemos venido describiendo y, por lo tanto, es difícil pensar en Huawei como un actor más en el mercado al estilo occidental, desvinculado completamente de los intereses del país al que pertenece.

En el terreno de la propiedad intelectual, las demandas contra Huawei han sido una constante prácticamente desde el inicio del presente siglo. Empresas como Cisco, T-Mobile, Motorola, Samsung, e incluso la también china ZTE, entre otras, han demandado a Huawei por infracción de derechos de propiedad intelectual y por robo de secretos industriales relacionado con diferentes productos.

Sobre los vínculos de la empresa con el ejército chino, han sido dos las principales causas de estas acusaciones. En primer lugar, el fundador y CEO de la compañía Ren Zhengfei sirvió en el ejército chino antes de iniciar la empresa y, por otra parte, la venta de equipos y tecnología a Irak e Irán ha sido vinculada por uno de los medios más influyentes de EEUU, *The Wall Street Journal*, al rastreo de disidentes por parte del gobierno iraní. Esta situación ha sido, como era de esperarse, rotundamente negada por Huawei (Tao, *et. al.* 2018).

Finalmente, uno de los principales temores en los EEUU sobre la inmersión de Huawei, y, en general, de las empresas tecnológicas chinas en sus mercados internos consiste en la amenaza a la seguridad nacional que supondría el uso de sus tecnologías y equipos con fines distintos a los meramente comerciales. Dicho de otra forma: el temor a que empresas como Huawei sean un medio para el espionaje o sabotaje que estaría impulsado por el gobierno chino, particularmente ante el inminente auge de la tecnología 5G, como se describe a continuación.

La tecnología 5G ocupa un lugar primordial en el marco de la competencia entre China-EEUU. Al respecto, Paul Triolo señala que: "en la disputa tecnológica entre Huawei y EEUU todo se trata de la batalla entre China y EEUU esencialmente, y Europa que también se ha involucrado, acerca de quién va a construir y operar la próxima generación de redes para telefonía móvil y para todos los dispositivos inteligentes. La llamada red 5G representa una arquitectura completamente nueva que permitirá velocidades realmente altas (…), pero más importante, permitirá nuevas aplicaciones como vehículos autónomos, realidad virtual (VR) y realidad aumentada (AR), cirugía remota, automatización industrial y está más pensada para comunicaciones entre máquinas que permitirán aplicaciones críticas para el futuro, por ejemplo, ciudades inteligentes" (Triolo, 2019).

La clave de la tecnología 5G radica en que los periodos de latencia que ofrecerá, es decir, los retrasos temporales en la propagación de datos en una red (el tiempo entre la transmisión de la información y su recepción), serán iguales o menores a un milisegundo, y

solo de esta forma se podrá asegurar el adecuado funcionamiento de las múltiples aplicaciones descritas por Triolo, entre muchas otras, incluyendo las relativas a Inteligencia Artificial (IA). Los vehículos autónomos, por ejemplo, requieren tener la capacidad técnica de reaccionar de manera casi inmediata; en medicina a distancia, la latencia entre robot y médico debe ser muy baja para evitar imprecisiones. Se trata pues de una tecnología que no debe ser vista como la evolución de la 4G, sino como un verdadero cambio de paradigma, una tecnología transversal que modificará la forma de producir, de transportar, de comercializar y de interrelacionarnos (Levy, 2019), de manera que se convierte en una tecnología de gran trascendencia para cualquier país. Por estas redes viajará no solo la información personal de su población, sino también los datos de infraestructura crítica (Triolo, 2019), de ahí la relevancia que tendrá la empresa que provea los equipos necesarios para su desarrollo en distintos países.

De esta forma, la tecnología 5G se está convirtiendo cada vez más en un campo de batalla geopolítico entre Estados Unidos y China (Ruhlig, 2019) y por primera vez en la historia moderna de China la creciente participación de mercado de Huawei y su habilidad tecnológica la están colocando en posición de dominar las tecnologías de siguiente generación (Johnson y Groll, 2019).

En ese sentido, han surgido diversas preocupaciones y acusaciones contra la empresa que se extienden a otras compañías de origen chino, por considerar que sus equipos podrían contener “puertas traseras” (*i.e.* códigos maliciosos), diseñadas para permitir a los espías chinos husmear en las comunicaciones o hasta tirar las propias redes. Esta idea ha permeado no solo en EEUU, sino también en algunos de sus aliados, que ya han adoptado medidas para limitar la adopción del kit de Huawei para el desarrollo de sus redes. Al respecto, uno de los principales argumentos de defensa de la compañía es que permitir las llamadas puertas traseras iría en contra de sus intereses comerciales, pues supondría poner en riesgo a sus clientes.

De hecho, Huawei indica que todas las acusaciones que ha hecho EEUU en su contra carecen de respaldo y evidencia, y que estarían dispuestos a formar parte de un diálogo, si es que hubiese seriedad en tratar de encontrar soluciones. En una reciente entrevista con Thomas Friedman, columnista de *The New York Times*, Ren Zhengfei le dijo: “Si Estados Unidos nos contacta de buena fe y promete cambiar su enfoque irracional hacia Huawei, entonces estamos abiertos a un diálogo. Estados Unidos no debería tratar de destruir a Huawei por algo trivial. Si EEUU siente que hemos hecho algo mal, entonces podemos discutirlo de buena fe y encontrar una solución razonable. Creo que podemos aceptar ese enfoque”, y añadió: "No hay restricciones sobre lo que estaríamos dispuestos a discutir con el Departamento de Justicia" (Friedman, 2019).

Ante este panorama, hay quienes afirman que en realidad la “guerra comercial de Trump no es sobre comercio, sino sobre tecnología” (Sheehan, 2018), pues tanto en el reporte del USTR conforme a la sección 301 de la Ley de Comercio, como en las medidas adoptadas desde su publicación “el objetivo principal es la política industrial china, dirigida a la mejora de su infraestructura tecnológica. Especialmente, las últimas acciones buscan combatir lo que es visto como esfuerzos concertados y coordinados por Beijing para adquirir tecnología americana en apoyo al plan *Made in China 2025*” (Sheehan, 2018). Nosotros vamos más allá, sin embargo: incluso la guerra tecnológica obedece a una

dinámica sistémica que le rebasa y que, por tanto, podría tener momentos de distensión como lo propone el fundador de Huawei, pero que, bajo las actuales circunstancias, probablemente tenderá a seguir escalando.

3. La participación de los gobiernos de ambas potencias en la disputa tecnológica

Muchos críticos de la posición estadounidense señalan que la motivación que mueve a Washington obedece sobre todo a la amenaza de perder el liderazgo tecnológico global. Aunque esta idea puede parecer razonable, también es cierto que la experiencia en el uso de tecnologías por parte del gobierno chino genera diversos cuestionamientos.

Durante los últimos años, distintos medios han reportado prácticas de espionaje por parte de instituciones del gobierno chino o de empresas presuntamente contratadas por éste. Por ejemplo, en julio de 2019 el diario británico *The Guardian* reportó que la policía fronteriza china, de forma secreta, había instalado aplicaciones de vigilancia en los teléfonos móviles de algunos visitantes, descargando información personal como parte del escrutinio intensivo del gobierno en la región remota de Xinjiang. Anteriormente, el mismo medio reportó que una empresa de vigilancia china había estado siguiendo los movimientos de al menos 2.5 millones de residentes en una provincia en la que minorías musulmanas han sido el objetivo de medidas drásticas de seguridad por medio de cámaras de circuito cerrado o dispositivos portátiles equipados con cámaras o *scanners* colocados en 6.7 millones de puntos de localización. Al respecto, en un estudio publicado recientemente, la organización *Human Rights Watch* reportó que la campaña del gobierno chino "*Strike Hard Campaign against Violent Terrorism*" ha convertido a Xinjiang en uno de los mayores centros chinos para el uso de tecnologías innovadoras para ejercer control social (Human Rights Watch, 2019).

Este tipo de actividades han generado una percepción de China como un estado de vigilancia en un sentido orwelliano y, como señala Sacks, esta percepción no está muy alejada de la realidad, pues el gobierno está usando tecnología de reconocimiento facial y *Big Data* para controlar y monitorear a sus ciudadanos. El incremento de este tipo de controles y el uso irrestricto de los datos personales por corporaciones chinas ha generado mayor conciencia entre la población acerca de su información personal en los últimos años, y detonó la respuesta del gobierno a través de legislación tendiente a la protección de datos personales de su población que[3], paradójicamente, cuenta ahora con más mecanismos de protección que en países como EEUU (Sacks, 2019) e incluso una de las más restrictivas a nivel mundial. Aún así, la mayoría de estos mecanismos son destinados a limitar el uso de esos datos únicamente por corporaciones, no por parte del gobierno.

En suma, se busca construir un régimen de protección de datos personales que se ajuste a los intereses de China, es decir, que genere confianza en una economía digital dinámica, pero que no interfiera con la capacidad del gobierno de mantener el control, lo cual es consistente con su modelo de gobernanza de internet (Sacks, 2019). Un estudio publicado recientemente por Oracle ha demostrado que la estructura del internet de China, a diferencia de cualquier otro país, es similar a una *Intranet* gigante. Esto quiere decir que "el país cuenta con muy pocos puntos de conexión con la red global de internet, tiene cero proveedores de telecomunicaciones extranjeros en su interior y el tráfico de internet China

[3] La Ley de Ciberseguridad China entró en vigor el 1 de junio de 2017.

a China nunca abandona sus fronteras. Todo esto le permitiría a China desconectarse del internet global si quisiera, y continuar operando, aunque sin conectividad a servicios occidentales" (Cimpanu, 2019).

Las preocupaciones relativas a las actividades de espionaje del gobierno chino a través de empresas de tecnología cobran mayor fuerza ante la posibilidad de que esta situación se extienda a otras latitudes y ha sido una de las principales causas de reacción en países occidentales, incluyendo por supuesto EEUU. Hasta ahora, no se ha generado evidencia significativa de que empresas chinas colaboren con el gobierno para realizar estas prácticas, aunque algunas acusaciones y reportes aislados sí apuntan en ese sentido. Por ejemplo, en Polonia un empleado chino de Huawei y un empresario polaco del ramo de ciber-negocios, fueron arrestados en enero de 2019 por autoridades locales bajo cargos de espionaje, aunque oficiales de ese país aclararon que se trataba de los individuos, no necesariamente relacionados con Huawei (The Guardian, 2019).

En otro reporte, algunos medios de República Checa han señalado que la división de Huawei en ese país, a través de sus empleados, es sospechosa de recolectar datos sensibles de oficiales y empresarios, obtenidos en reuniones de negocios y aprovechando su relación como clientes de la compañía. Estos datos habrían sido ingresados a una base de datos central a la que tendrían acceso las oficinas principales de la compañía en China, además de que la información habría sido discutida en reuniones de la empresa con representantes de la embajada China en República Checa (MacEnchroe y Kroupa, 2019).

Uno de los principales detonantes de la gran inquietud en materia de seguridad nacional en Occidente ha sido la Ley de Seguridad Nacional China, que entró en vigor el 27 de junio de 2018 y se actualizó en abril de 2019. Dicha ley requiere de todas las organizaciones y ciudadanos de China, apoyar, asistir y cooperar con los trabajos de inteligencia nacional, así como mantener secretos los trabajos de inteligencia de los que tengan conocimiento. De acuerdo con analistas, esta ley sería aplicable globalmente a corporaciones chinas, incluyendo subsidiarias que se encuentren basadas fuera de China (Manheimer Swartling, 2019), y por ello se sospecha que estas empresas tendrían que abrir las "puertas traseras" para el gobierno chino.

A la luz del panorama descrito es que deben entenderse las medidas adoptadas por EEUU en su disputa comercial con China, como la imposición de tarifas arancelarias a ciertos productos y otras acciones restrictivas al comercio bilateral. Estas tienen un trasfondo que, como hemos sostenido en este texto, va mucho más allá del comercio. Basta con analizar la primera medida formal adoptada por el gobierno estadounidense en relación con prácticas comerciales chinas, materializada en la "*Investigación sobre los actos, políticas y prácticas chinas, relacionadas con transferencia tecnológica, propiedad intelectual e innovación, de acuerdo con la sección 301 de la Ley de Comercio de 1974"* que, esencialmente, se refiere a cuatro tipos de conductas desarrolladas por el gobierno chino:

(i) **Régimen de transferencia tecnológica china**, que afirma que las autoridades de ese país han exigido a las firmas extranjeras formar *Joint Ventures* con empresas nacionales y, de esta forma, transferir propiedad intelectual sumamente valiosa, como requisito para operar en China. Estas prácticas fueron particularmente onerosas en industrias asociadas a *Made in China 2025* (Sheehan, 2018).

(ii) **Prácticas de licenciamiento discriminatorio de China**, que se refiere a la legislación China a través de la cual se priva a los propietarios de tecnología de EEUU, de la posibilidad de negociar y fijar los términos de transferencias tecnológicas sin la intervención gubernamental China, necesaria para otorgar autorizaciones administrativas. De acuerdo con Sheehan, un ejemplo de este tipo de prácticas es la regla consistente en que, una vez cumplidos 10 años de pagar por el licenciamiento, la firma china podría usar la tecnología a perpetuidad, después de que el contrato finalice.

(iii) **Régimen de inversión china en el extranjero**, representado por la estrategia denominada "*Going Out*" –que se podría traducir como "Salir de Compras"– mediante la cual el gobierno chino fomenta que las empresas de ese país inviertan en el extranjero y ofrece apoyos dirigidos específicamente a ciertos sectores, como circuitos integrados, tecnologías de la información e inteligencia artificial. Sobre la estrategia "*Going Out*", señala Sheehan, muchas de estas adquisiciones se refieren a apoyos gubernamentales que actúan en contra de las fuerzas del mercado o les otorgan a empresas chinas múltiples ventajas para superar las ofertas de otros compradores.

(iv) **Intrusiones chinas no autorizadas a redes de cómputo estadounidenses y robo ciber-habilitado (*i.e. hacking*) de propiedad intelectual e información comercial sensible**, en donde los objetivos principales serían corporaciones estadounidenses que se encuentran en el marco de las industrias relacionadas con el *Plan Made In China 2025* (Sheehan, 2019).

Finalmente, aunque no forma parte medular de la investigación, también se apuntan algunas actividades relacionadas con la seguridad nacional y la ciberseguridad, particularmente los riesgos que la Ley de Ciberseguridad de la República Popular China (Ley de Ciberseguridad de 2017) supondría en esta materia. En suma, las empresas estadounidenses manifestaron preocupaciones sobre las revisiones de seguridad para una amplia gama de productos de tecnologías de la información, las restricciones al flujo de datos que crucen la frontera de China (hacia fuera), requerimientos de localización de ciertos tipos de datos o personas, y el desarrollo de estándares de ciberseguridad nacionales que excederían el alcance de estándares internacionales, actividades que estarían fomentadas por la Ley de Ciberseguridad de 2017.

Este reporte detonó diversas acciones por parte del gobierno de EEUU que continúan a la fecha e incluyen la imposición de aranceles a productos chinos principalmente relacionados con *Made in China 2025*, restricciones a las inversiones chinas en los EEUU y la presentación de una queja ante la Organización Mundial del Comercio, que busca combatir los derechos que otorga la legislación China para usar tecnología extranjera a perpetuidad después de un periodo de licenciamiento de 10 años. Sin embargo, algunos autores consideran que el foco que se ha fijado en la imposición de aranceles pudiera representar una victoria pírrica para la administración de Trump, pues mientras se reduce el déficit comercial, se podrían desatender cuestiones más profundas relacionadas con la adquisición de tecnología por parte de empresas chinas (Sheehan, 2019) o con el uso de esa tecnología en detrimento de la seguridad nacional.

Aquí, es importante considerar que los retos que se presentan para el gobierno estadounidense ante los riesgos advertidos en el uso de tecnología china obedecen a un contexto sumamente complejo en el terreno geopolítico descrito en los primeros apartados

de este trabajo, particularmente porque un bloqueo o *bypass* comercial sobre China podría realizarse, pero solo pagando un enorme costo (The Economist, 2019). Lo que señala Sacks (2019) viene muy a cuento de lo que hablábamos anteriormente en términos de la interdependencia y vinculación de ambas economías:

> *"EEUU y China pertenecen a un sistema interconectado en cuanto a investigación, desarrollo, manufactura y talento. La innovación de empresas americanas se ve favorecida por su acceso al mercado chino. Los fabricantes líderes de semiconductores generan ganancias substanciales en China y posteriormente destinan una gran porción de esas ganancias de regreso en investigación y desarrollo con la finalidad de mantenerse competitivas en tecnologías emergentes como 5G. A diferencia de la carrera espacial en la Guerra Fría con la Unión Soviética, la línea entre China y Estados Unidos en desarrollo tecnológico no es tan clara como la frontera política entre los dos países. Esfuerzos por segregar o 'desemparejar' los dos sistemas vendrán con un enorme costo para la innovación y el liderazgo tecnológico de los Estados Unidos"*

La disputa China – EEUU alcanzó uno de sus puntos más álgidos el 1 de diciembre de 2018 cuando Meng Wanhzhou, hija del fundador de Huawei y Directora Financiera de la compañía, fue arrestada en Canadá a solicitud del Departamento de Justicia de EEUU bajo la sospecha de que había colaborado con la compañía en actividades fraudulentas para evadir sanciones impuestas por EEUU a Irán, lo que generó además tensiones entre China y Canadá que se han extendido hasta la fecha. Tan solo unos meses después, algunas empresas estadounidenses también adoptaron acciones destinadas a limitar el acceso a sus productos por parte de Huawei, principalmente Google, quien en mayo de 2019 anunció que suspendería los negocios con Huawei que requirieran transferencia de software o hardware a la empresa china, con lo que restringió el uso de su sistema operativo Android en los equipos de Huawei, medida que siguieron otras empresas dedicadas a la creación de microprocesadores, como Qualcomm, Broadcom e Intel, entre otras (King, *et al*. 2019).

Sin embargo, no solo Canadá y las empresas estadounidenses han entrado al escenario de la disputa entre EEUU y China, pues gobiernos de otros países también han adoptado medidas restrictivas a productos chinos o, al menos, los han puesto en la mira a partir de las acusaciones estadounidenses, aunque las razones para hacerlo han sido distintas a las meramente comerciales, como se analizará en el siguiente apartado.

4. Reacciones en otros países

a. Reino Unido

A la par del surgimiento y evolución de la disputa comercial entre EEUU y China y con un enfoque centrado en riesgos a la seguridad nacional, en Reino Unido se creó desde 2010 un "Centro de Evaluación de la Ciberseguridad de Huawei" ("HCSEC" por sus siglas en inglés), a partir de una serie de acuerdos entre la empresa y el gobierno británico, con la finalidad de mitigar cualquier riesgo que se perciba derivado del involucramiento de

Huawei en aspectos de la infraestructura crítica nacional del Reino Unido. La Junta de Supervisión del HCSEC es presidida por el Director General del Centro de Ciberseguridad Nacional (*i.e.* la agencia gubernamental de operaciones líder en ciberseguridad del Reino Unido) y participa un ejecutivo de alto nivel de Huawei como vicepresidente, así como diversos representantes de alto nivel, tanto del gobierno como de la industria de telecomunicaciones británica.

El HCSEC ha producido cinco reportes anuales con la evaluación de una gama de productos de Huawei que se emplean en los mercados de telecomunicaciones del Reino Unido, el último de ellos publicado el 28 de marzo de 2019 en el que dicho órgano concluyó, *inter alia*, que se han identificado cuestiones técnicas relevantes en los procesos de ingeniería de Huawei que representan nuevos riesgos para las redes de telecomunicaciones del Reino Unido, además de que no se ha logrado progreso significativo en la reparación de los riegos reportados el año anterior.

Tomando en cuenta lo señalado, el HCSEC sostiene que, en tanto los defectos de ingeniería de software de Huawei como sus procesos de ciberseguridad sean remediados y considerando el contexto de despliegue (de redes) que experimenta el Reino Unido, sería difícil gestionar apropiadamente los riesgos de productos futuros de la empresa. Por lo tanto, el organismo afirmó que solo puede ofrecer una garantía limitada de que todos los riesgos a la seguridad nacional derivados del involucramiento de Huawei en redes críticas podrán ser mitigados en el largo plazo.

El reporte del HCSEC inició una serie de discusiones sobre el camino que debería tomar el Reino Unido en relación con los productos chinos y algunos medios reportaron posteriormente que la entonces primera ministra británica, Theresa May, habría ordenado en una reunión con su Consejo de Seguridad Nacional, el veto a ciertos productos de Huawei para su comercialización en Reino Unido. Sin embargo, ante los movimientos políticos que han tenido lugar en esa nación en los últimos meses, la decisión final es aún incierta.

b. Unión Europea

Tan solo un par de días previos a la publicación del reporte del HCSEC de Reino Unido, la Comisión Europea emitió un comunicado en el que recomienda una serie de acciones operativas y medidas para asegurar en la Unión Europea (UE) un alto nivel de ciberseguridad de las redes 5G, el cual parte de una resolución del Parlamento Europeo aprobada el 12 de marzo de 2019 sobre amenazas a la seguridad relacionadas con el crecimiento de la presencia tecnológica china en la UE. Lo anterior, en el marco de la aprobación de una Ley de Ciberseguridad por parte del Parlamento Europeo, que tuvo lugar en la misma fecha.

Tales recomendaciones se dividieron en dos materias, fundamentalmente. Primero, la UE recomendó que, a nivel nacional, los estados deberían realizar para finales de junio de 2019 una evaluación de riesgos en relación con las infraestructuras de red de 5G, así como actualizar los requisitos actuales para los proveedores y operadores involucrados.

En segundo lugar, la Comisión Europea recomendó que, a nivel regional, se debería intercambiar información entre los países que conforman la UE y que, con el apoyo de la propia Comisión y de la Agencia Europea para la Ciberseguridad, creada desde 2004, se

debería completar una evaluación de riesgos coordinada, en octubre de 2019. A partir de la evaluación, una serie de medidas de mitigación de riesgos podrían adoptarse en el plano nacional.

c. Nueva Zelanda y Australia

Otros países también han adoptado medidas restrictivas en relación con equipos chinos, particularmente de Huawei, para el desarrollo de redes 5G. Tal es el caso de Nueva Zelanda que, a través de su agencia de inteligencia, rechazó en noviembre de 2018 la solicitud de Spark New Zealand Ltd., proveedor de servicios de telecomunicaciones, de emplear equipos de tecnología 5G de la compañía china, bajo argumentos de seguridad nacional (Greenfield, 2018).

De igual forma, Australia había prohibido desde agosto de 2018 la participación de Huawei en la construcción de redes 5G en ese país, argumentando también razones de seguridad nacional, al señalar que "el involucramiento de fabricantes que podrían estar sujetos a instrucciones extrajudiciales de un gobierno extranjero, en conflicto con la legislación Australiana, podrían poner en riesgo a los proveedores de servicios de fallar en la adecuada protección de las redes 5G de cualquier intervención o acceso injustificado" (Ministerio de Comunicaciones Australianas, 2018). Al respecto, vale la pena decir que en 2017 el gobierno australiano implementó un nuevo marco jurídico con el objetivo de que las agencias de seguridad y la industria de telecomunicaciones compartieran información sensible relacionada con amenazas a las redes de telecomunicaciones (las Reformas al Sector de Telecomunicaciones en materia de Seguridad).

c. Japón

Otro gobierno que se sumó a las restricciones a empresas de origen chino fue el japonés que, en diciembre de 2018, prohibió el uso de determinados equipos en las adquisiciones del sector público, con la finalidad de evitar fugas de información sensible derivadas de funcionalidades con intención maliciosa. Aunque las disposiciones implementadas no mencionan específicamente a alguna empresa, las más afectadas fueron Huawei y ZTE.

En conclusión, la expansión tecnológica China y la inminente llegada de la tecnología 5G, han detonado llamados a proteger la ciberseguridad en el plano nacional y regional e incluso algunos autores consideran que ya debería de plantearse la creación de un sistema de monitoreo global en esta materia (Triolo, 2019), similar a la Agencia Internacional de Energía Atómica (IAEA por sus siglas en inglés).

5. El Caso de América Latina

En América Latina la discusión sobre ciberseguridad no ha madurado tanto como en otras regiones del mundo y los esfuerzos de protección en la materia son apenas esbozos, en muchos casos desarticulados, tanto internamente como hacia el exterior. Sin embargo, la inversión de empresas de origen chino en esta zona continúa incrementándose y el mercado es todavía muy amplio.

Huawei es la empresa que más proyectos obtuvo para construir infraestructura 4G en la región (Cote-Muñoz & Lorand, 2019). El caso argentino es paradigmático en este sentido pues las empresas de origen chino (Huawei y ZTE) alcanzaron un rápido crecimiento en ese

país al proveer servicios en mercados rurales poco competitivos. De ahí se abrieron camino hacia zonas urbanas y, en poco años, lograron ganancias en el mercado argentino y se convirtieron en proveedoras de equipos para monopolios clave que se alinearon hace algunos años con los intereses chinos en el mercado, desplazando con ello a empresas estadounidenses que, incluso, han decidido dejar ese país (Hulse, 2007).

En materia de ciberseguridad, los datos muestran que la región latinoamericana todavía no cuenta con la fortaleza necesaria. Por ejemplo, en 2017 América Latina sufrió 667 millones de ciberataques, 57% más que en el año anterior, lo que le costó a la región $97 billones de dólares (Cote-Muñoz y Lorand, 2019). Al respecto, durante el mismo año México fue el tercer país del mundo que recibió más ciberataques y el primer lugar de América Latina, lo que reflejó una pérdida de 7,700 millones de dólares (Lockton, 2019).

Esto colocaría a la región latinoamericana en una situación de vulnerabilidad muy particular, si asumimos que las amenazas que se han planteado en EEUU y otros países en el uso de equipos chinos son reales.

La relevancia del tema quedó clara en una investigación de *The Wall Street Journal* del 14 de agosto de este año (Parkinson, Barrivo y Chin, 2019). Según ese reporte, algunos técnicos de Huawei han estado colaborando con ciertos gobiernos en África para espiar a sus opositores políticos. También asegura que, en países como Uganda o Zambia, los técnicos de Huawei ayudaron a los servicios de seguridad nacional y a los reguladores de telecomunicaciones a penetrar en redes como WhatsApp o páginas de Facebook a fin de determinar sus ubicaciones y espiar en los planes de actividades políticas de dichos opositores. Huawei, una vez más, negó las acusaciones.

No obstante, es indispensable comprender de qué estamos hablando. Si los riesgos para países más industrializados siguen siendo enormes, aunque han tomado medidas preventivas desde hace años, pensemos qué sucede en países y sociedades como las de nuestro subcontinente, que mayormente carecen de la preparación para resistir ese tipo de vulnerabilidades, las cuales tienden a potenciarse bajo condiciones de corrupción e impunidad. El control de las redes de comunicación e información no es un tema menor. Los reportes y señales que apuntan hacia el uso de la tecnología para avanzar determinados intereses estratégicos en el medio de una disputa mayor, se siguen sumando.

6. México.

Huawei está presente en México desde 2001 (Micheli y Carrillo, 2016) y su crecimiento en el país ha sido acelerado en los últimos años. Tan solo en el mercado de teléfonos móviles, entre 2014 y 2016 pasó de contar con una participación de mercado de 4.1 a 9.1 por ciento (Select, 2019). Actualmente se disputa el segundo lugar en este rubro con Motorola, y sus directivos afirman que durante el primer semestre de 2019 ha tenido una tasa de crecimiento de ventas de 128 por ciento, comparado con el mismo periodo del año anterior (Forbes, 2019).

En cuanto al mercado de infraestructura para redes, algunos reportes indican que junto con Cisco y Ericsson, Huawei es uno de los principales proveedores de esta infraestructura en México, un mercado que muestra tasas de crecimiento de 7 por ciento anual (El Economista, 2019) que podrían aumentar ante el inminente despliegue de redes 5G, un tema que cada vez comienza a tomar más fuerza en nuestro país.

La discusión sobre el despliegue de redes 5G en México ha sido impulsada principalmente por el regulador nacional de las telecomunicaciones, el Instituto Federal de Telecomunicaciones (IFT), que ha iniciado una serie de acciones relacionadas, sobre todo, con la definición de las bandas del espectro radioeléctrico que serán susceptibles de aprovechamiento para este tipo de redes.

Huawei ha estado presente y activo a lo largo de estas discusiones. Por ejemplo, durante abril de 2018 se realizó el seminario "Visiones de la industria relativas al espectro radioeléctrico para sistemas 5G" organizado por el IFT, en el que participaron representantes de Ericsson, Nokia, Huawei, Qualcomm e Intel (IFT, 2018) y más recientemente, en mayo de 2019, representantes de Huawei sostuvieron una reunión con los Comisionados del IFT que tuvo como tema central la "Planeación del espectro radioeléctrico, redes 5G y bandas que integrarán este ecosistema" así como los resultados de un estudio elaborado por el regulador en esta materia (IFT, 2019), lo que muestra el interés de la empresa por participar en el desarrollo de la infraestructura.

A pesar de que México empieza a preparar el camino para el despliegue de redes 5G, la discusión sobre sus implicaciones en materia de ciberseguridad, los riesgos que ello implica y la forma de limitarlos, no ha cobrado mayor fuerza. Tampoco han existido pronunciamientos sobre los parámetros de seguridad que deberán observar las empresas que quieran participar en el desarrollo de estas redes, mucho menos sobre la participación de alguna empresa en particular.

En materia de política de ciberseguridad en México, uno de los principales esfuerzos se dio en 2017, cuando el gobierno federal presentó un documento denominado "Estrategia Nacional de Ciberseguridad" que ofrecía la "visión del Estado mexicano en la materia" y que recogía los resultados de distintos foros y estudios elaborados por diversas instituciones, tanto públicas como de la industria. Sin embargo, el hecho de que se haya presentado hacia finales del sexenio pasado y el cambio de gobierno y de partido político en el poder que tuvo lugar en 2018, generaron que esta estrategia se diluyera.

Durante la presente administración, a través de la Secretaría de Comunicaciones y Transportes se elaboró un "Simulador de Ciberseguridad" que tiene el objetivo de "generar conciencia acerca del uso responsable y seguro de las tecnologías" dirigido sobre todo a los usuarios de TICs.

Por otra parte, el IFT publicó un documento denominado Visión Regulatoria de las Telecomunicaciones y la Radiodifusión 2019 – 2023 que, en el apartado "Desarrollo de Internet y Regulación de Telecomunicaciones en el Ecosistema Digital", incorpora una sección de Ciberseguridad en el que anticipa de manera genérica algunos de los principales retos regulatorios en esta materia, incluyendo la necesidad de actualizar la "estrategia integral de ciberseguridad" (IFT, 2018), sin profundizar mucho al respecto.

Posteriormente, el IFT publicó un "Plan de Acciones en Materia de Ciberseguridad" en el que anticipa la posibilidad de emitir lineamientos técnicos relativos a la infraestructura y a los equipos que hacen uso del espectro radioeléctrico o que se conectan a redes de telecomunicaciones; sin embargo, también se refiere a la necesidad de que otras autoridades (*i.e.* Secretarías del Ejecutivo Federal, INAI) participen activamente en el ámbito de sus facultades en la emisión de disposiciones asociadas a la ciberseguridad.

En suma, hasta ahora se han dado algunos esfuerzos aislados y desarticulados en materia de cibserseguridad por parte de diversas instituciones del Estado Mexicano, pero no podemos hablar todavía de una estrategia integral en esta materia, con objetivos definidos, líneas de acción claras y métricas establecidas, lo que se ha reflejado en algunos indicadores internacionales que evalúan este rubro.

Al respecto, de acuerdo con el Índice Global de Ciberseguridad de la Unión Internacional de Telecomunicaciones (UIT), que mide el nivel de compromiso de 194 países en la materia, entre 2017 y 2018 México cayó del lugar 28 de 193 al lugar 63 y a nivel lationoamerica pasó de liderar la región al segundo lugar, pues fue superado por Uruguay. Sin embargo, lo que más llama la atención es la enorme brecha existente entre nuestro país y EEUU y Canadá que ocupan el lugar 2 y 9 respectivamente (UIT, 2019).

El Índice de la UIT está basado en 5 pilares: legal, técnico, organizacional, desarrollo de capacidades y cooperación y conforme al reporte para el año 2017 las fortalezas en nuestro país están asociadas al ámbito legal, que evalúa la existencia de legislación en materia de ciber-delincuencia, protección de datos personales, privacidad y transacciones electrónicas, mientras que las evaluaciones más bajas las obtuvo en cooperación y el aspecto organizacional, debido a la falta de acuerdos bilaterales y multilaterales, así como la falta de estrategia, entre otros factores.

El contexto descrito es una clara muestra de la necesidad de implementar, cuanto antes, una estrategia nacional de ciberseguridad que incluya parámetros claros para cualquier empresa que pretenda participar en el despliegue de redes 5G en México, entre otros elementos.

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

- La rivalidad entre Estados Unidos y China refleja una realidad probablemente diferente a momentos de la historia que eran descritos por conceptos como la "competencia entre grandes poderes" o "Guerra Fría". Estamos ante condiciones distintas en las que la competencia y el conflicto geopolítico estructural se ven obligados a coexistir con la interdependencia y la cooperación.

- No obstante, el estar tomando medidas que buscan desvincular a ambas economías (lo que incluye, pero no se limita a lo comercial), sobre todo si se suma a otros aspectos de la confrontación geopolítica, está activando una espiral conflictiva que va adquiriendo su propia dinámica, la cual se manifiesta desde múltiples esferas.

- De manera notable, estamos ante una importante escalada tanto de ciberataques como de la guerra informativa entre las superpotencias. La enorme dependencia de la tecnología vuelve a empresas, organizaciones y agencias públicas, pero también a la población, altamente vulnerables ante este tipo de ataques.

- No es casualidad que la disputa entre EEUU y China tenga en las cuestiones tecnológicas uno de sus mayores componentes; el futuro de las sociedades estará definido en buena medida por su capacidad de adaptarse a sociedades hiperconectadas que, al mismo tiempo, ofrezcan seguridad a sus ciudadanos, garanticen los principios democráticos y preserven los derechos humanos.

- Lo señalado hasta ahora pone los focos rojos sobre la fragilidad que en Latinoamérica y específicamente en México tenemos por encontrarnos expuestos, sin la suficiente protección y preparación, en medio de un conflicto de dimensiones mayúsculas que, como se dijo, tiene en la tecnología uno de sus componentes esenciales.

- Fuera de EEUU, las causas para justificar restricciones a productos y tecnologías provenientes de China, se han basado más en aspectos como la seguridad nacional y riesgos a la ciberseguridad, que en aspectos comerciales y prácticas cuestionables en un contexto de apertura comercial.

- Un escenario de segregación de la economía China del resto del mundo, a estas alturas, parece poco probable. La cuestión será definir el nivel de participación de empresas chinas en la economía mundial y, particularmente, los riesgos de dicha participación para la evolución de los mercados, la seguridad y la innovación.

- Considerando la experiencia internacional, es innegable que la presencia de tecnología china en el despliegue y operación de redes de telecomunicaciones, particularmente 5G, implica riesgos a la seguridad nacional. Sin embargo, lo mismo

podría decirse de cualquier otro gobierno o país que se involucre directamente en este despliegue. Cualquier medida al respecto debe ser, entonces, adoptada considerando las particularidades de los proveedores y las vulnerabilidades identificadas en el país que corresponda.

- México ocupa una posición estratégica en la disputa comercial entre EEUU y China; sin embargo, debe ser sumamente cauteloso pues hay algunos valores fundamentales involucrados que pudieran verse comprometidos a cambio de una ventaja o apalancamiento comercial, como la seguridad, la privacidad, los datos personales e, incluso, la propia relación con EEUU.

- No se observa, a la fecha, que la ciberseguridad sea un tema que se encuentre en la agenda pública en México. Las principales discusiones en el país en materia de despliegue de redes 5G se han centrado en aspectos comerciales; hasta ahora, el componente de seguridad nacional aparece de manera muy marginal.

- Las agencias de ciberseguridad a nivel nacional y regional comienzan a propagarse; es muy probable que, por la naturaleza de los riesgos y la esencia de la sociedad digital, las soluciones se deban analizar regional y globalmente. No obstante, es importante que cada país considere y plantee sus particularidades en estas discusiones, para lo cual se requiere una verdadera política de Estado en la materia.

- Considerando lo anterior, es indispensable estudiar y evaluar las condiciones bajo las que nuestro entorno particular se encuentra y los riesgos que debe enfrentar. Este tema se entreteje con otras cuestiones estructurales tales como la corrupción, la debilidad del estado de derecho o la elevada impunidad, condiciones que incrementan el peligro de que distintos actores saquen partido de nuestra posición para avanzar sus propias agendas. Es natural pensar que, bajo las circunstancias estructurales que definen a países como el nuestro, las vulnerabilidades crecen. De ahí que proponemos las siguientes recomendaciones.

Recomendaciones

- Una aproximación de "*esperar y ver"* lo que sucede en otros países en materia de seguridad nacional derivada de la presencia de tecnologías chinas en el despliegue de redes de telecomunicaciones no es la opción más recomendable en México o cualquier otro país que se encuentre actualmente al margen de la disputa. La presencia y expansión de empresas tecnológicas chinas es una realidad y deben adoptarse acciones.

- Considerando el contexto analizado y las particularidades de México, un enfoque de participación de múltiples partes (*multistakeholder*) para atender las cuestiones relacionadas con presencia tecnológica china en México, pudiera ser lo más recomendable por lo pronto, algo similar a lo sucedido en Reino Unido con el HCSEC.

- Por el momento, una aproximación basada en riesgos pudiera ser la más apropiada para atender los cuestionamientos derivados de la presencia y expansión tecnológica china en México.

- En las decisiones de política pública asociadas al despliegue de redes 5G, el componente de seguridad nacional debe ser considerado, con independencia de las empresas que pueden ofrecer equipos para la operación de dichas redes.

- La CPEUM ya establece como principio de política pública la prohibición de injerencias arbitrarias en la prestación de servicios de telecomunicaciones (Artículo 6º). Aunque quizás no se anticipaba en el contexto actual, este principio se debe hacer valer por las autoridades en México.

- Debe iniciarse cuanto antes el análisis de la probable creación de un esquema de certificación de ciberseguridad aplicable a México, que involucre a distintas autoridades y la participación de todos los interesados.

- Deben definirse las tareas de cibserseguridad necesarias para el país y establecer la autoridad o autoridades que estarán a cargo de dichas labores de manera articulada. Por lo pronto, no nos pronunciamos sobre el modelo institucional más apropiado pues deben analizarse diversos factores, pero es necesario iniciar la discusión cuanto antes.

- Ante el contexto internacional, el tema de ciberseguridad, particularmente en redes 5G, puede ser uno que se atienda mejor de manera regional, los países latinoamericanos comparten características comunes que podrían propiciar acciones y posiciones coordinadas en beneficio de todos.

- En México, debe analizarse la creación de un marco jurídico en materia de ciberseguridad que sea uniforme y aplicable en todos los niveles de gobierno, sin que ello implique límites rígidos a la innovación o el desarrollo de los mercados.

- Crear una normatividad común en ciberseguridad es una de las medidas necesarias para evitar un conflicto directo entre países. Establecer normas regionales puede delimitar las acciones de empresas extranjeras en Latinoamérica, facilitando sanciones y reglas.

Referencias

Boland, Hannah. 2019. Theresa May's resignation delays final decision on using Huawei in Britain's 5G networks. *The Telegraph*, 30 de mayo de 2019. https://www.telegraph.co.uk/technology/2019/05/30/theresa-mays-resignation-delays-final-decision-using-huawei/ (Consultado el 6 de septiembre de 2019)

Bradsher, Keith. 2019. Next Made in China Boom: College Graduates. *The New York Times*. Enero 16, 2013. https://www.nytimes.com/2013/01/17/business/chinas-ambitious-goal-for-boom-in-college-graduates.html (Consultado el 15 de agosto de 2019)

Cimpanu, Catalin. 2019. Oracle: China's internet is designed more like an intranet. Julio 23 de 2019. *Zero Day*. https://www.zdnet.com/article/oracle-chinas-internet-is-designed-more-like-an-intranet/ (Consultado el 2 de septiembre de 2019)

Cote-Muñoz, N y Laskai, L. 2019. Is Latin America Prepared for China's Booming Tech Investments? *America Quarterly*. https://www.americasquarterly.org/content/chinese-companies-are-betting-latin-american-tech-players (Consultado el 6 de septiembre de 2019)

Cyrril, Melissa**.** 2018. What is Made in China 2025 and Why Has it Made the World So Nervous? Diciembre 28, 2018. *China Briefing*. https://www.china-briefing.com/news/made-in-china-2025-explained/ (Consultado el 19 de agosto de 2019)

Chen, Eliot. "Made in China 2025" Unmade? Macro Polo. Agosto 20, 2019. https://macropolo.org/analysis/made-in-china-2025-dropped-media-analysis/ (Consultado el 3 de septiembre de 2019).

Denyer, Simon. 2019. Japan effectively bans China's Huawei and ZTE from government contracts, joining U.S. *The Washington Post*, 10 de diciembre de 2018. https://beta.washingtonpost.com/world/asia_pacific/japan-effectively-bans-chinas-huawei-zte-from-government-contracts-joining-us/2018/12/10/748fe98a-fc69-11e8-ba87-8c7facdf6739_story.html?noredirect=on (Consultado el 6 de septiembre de 2019)

Departamento del Tesoro de los EEUU. 2019. "US Gross External Debt". https://bit.ly/2LvBAPv (Consultado el 1 de mayo de 2019).

El Economista. Huawei, en el top de proveedores de centros de datos y fabricantes TIC en México. 20 de mayo de 2019. https://www.eleconomista.com.mx/tecnologia/Huawei-en-el-top-de-proveedores-de-centros-de-datos-y-fabricantes-TIC-en-Mexico-20190520-0044.html (Consultado el 23 de septiembre de 2019)

European Commission. 2018. EU negotiators agree on strengthening Europe's cybersecurity. 11 de diciembre de 2018. https://ec.europa.eu/commission/news/cybersecurity-act-2018-dec-11_en (Consultado el 5 de septiembre de 2018).

European Commission. 2019. The Cybersecurity Act strengthens Europe's cybersecurity. 19 de marzo de 2019. https://ec.europa.eu/digital-single-market/en/news/cybersecurity-act-strengthens-europes-cybersecurity (Consultado el 6 de septiembre de 2019).

Expansión. 2019. México es el tercer país en América Latina con mayor crecimiento de ciberataques. https://expansion.mx/tecnologia/2018/12/11/mexico-es-el-tercer-pais-en-america-latina-con-mayor-crecimiento-de-ciberataques (Consultado el 6 de septiembre de 2019).

Federal Reserve Bank of Minneapolis. 2016. China's Foreign Investment. Economic Policy Papers. https://www.minneapolisfed.org/research/economic-policy-papers/chinas-foreign-investment (Consultado el 10 de septiembre de 2019)

Forbes. Huawei crece en el mercado mexicano y busca el trono del primer lugar. Agosto 5 de 2019. https://www.forbes.com.mx/huawei-sigue-remontando-en-el-mercado-mexicano-y-busca-el-trono-del-primer-lugar/ (Consultado el 23 de septiembre de 2019)

Friedman, Thomas. 2019. Huawei Has a Plan to Help End Its War With Trump. The New York Times. https://www.nytimes.com/2019/09/10/opinion/huawei-trump-china-trade.html (Consultado el 11 de septiembre de 2019):

Gobierno de México. Estrategia Nacional de Ciberseguridad, México 2017. https://www.gob.mx/cms/uploads/attachment/file/271884/Estrategia_Nacional_Ciberseguridad.pdf (Consultado el 23 de septiembre de 2019)

Gómez, Esther. 2016. Plan Made in China 2025. Oficina Económica y Comercial de la Embajada de España en Pekin. Octubre, 2016

Gracefo, A. 2019. China's National Champions: State Support Makes Chinese Companies Dominant. *Foreign Policy Journal*, Mayo 15 de 2017. https://www.foreignpolicyjournal.com/2017/05/15/chinas-national-champions-state-support-makes-chinese-companies-dominant/ (Consultado el 27 de agostro de 2019)

Greenfield, Charlotte. 2018. Nueva Zelanda rechaza el uso del 5G de Huawei alegando motivos de seguridad nacional. *Reuters*, 28 de noviembre de 2018. https://lta.reuters.com/articulo/worldNews/idLTAKCN1NX0VI-OUSLW

Guilford, Gwynn y Dan KopfJune . 2019. The trade war is already pushing businesses out of China—and it could be permanent. *Quartz*. https://qz.com/1641598/trumps-trade-war-with-china-is-reshaping-global-trade/ (Consultado el 12 de septiembre de 2019).

HCSEC Anual Report 2019. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/790270/HCSEC_OversightBoardReport-2019.pdf (Consultado el 4 de septiembre de 2019).

Heatley, Jesse. Xi Doubles Down on China's Cyber Goals and Semiconductor Plans. The Diplomat, Abril 26, 2018. https://thediplomat.com/2018/04/xi-doubles-down-on-chinas-cyber-goals-and-semiconductor-plans/ (Consultado el 4 de septiembre de 2019)

Herrasti, Gonzalo. El riesgo de ciberataques, una realidad palpable. Lockton. Diciembre, 2018. http://www.lockton.com.mx/Website/media/10417/whitepaper-cyber-1.pdf (Consultado el 5 de septiembre de 2019)

Hudson Institute. 2018. "Vice-President Mike Pence's Remarks on the Administration's Policy Towards China", Discurso pronunciado el 4 de octubre de 2018. https://bit.ly/2y15lz7 (Consultado el 12 de septiembre de 2019).

Hulse, Janie. 2019. China's Expansion into and U.S. Withdrawal from Argentina's Telecommunications and Space Industries and the Implications for U.S. National Security**.** Septiembre, 2017. https://www.globalsecurity.org/military/library/report/2007/ssi_hulse.pdf (Consultado el 6 de septiembre de 2019)

Human Rights Watch. 2019. **China's Algorithms of Repression,** Reverse Engineering a Xinjiang Police Mass Surveillance App. Mayo 1 de 2019. https://www.hrw.org/report/2019/05/01/chinas-algorithms-repression/reverse-engineering-xinjiang-police-mass-surveillance (Consultado el 30 de agosto de 2019)

Instituto Federal de Telecomunicaciones. 2018. El Instituto Federal de Telecomunicaciones lleva a cabo seminarios de espectro para sistemas 5G (Comunicado 29/2018) 12 de abril de 2018. http://www.ift.org.mx/comunicacion-y-medios/comunicados-ift/es/el-instituto-federal-de-telecomunicaciones-lleva-cabo-seminarios-de-espectro-para-sistemas-5g (Consultado el 23 de septiembre de 2019)

Instituto Federal de Telecomunicaciones. 2018. Plan de Acciones en Materia de Ciberseguridad. Noviembre 2018. Versión 3. http://www.ift.org.mx/sites/default/files/contenidogeneral/transparencia/upr-planaccionesciberseguridad.pdf (Consultado el 20 de septiembre de 2019)

Instituto Federal de Telecomunicaciones. 2018. Visión regulatoria de las telecomunicaciones y la radiodifusión, 2019-2023. Septiembre, 2018. http://www.ift.org.mx/sites/default/files/contenidogeneral/transparencia/1vision19-23.pdf (Consultado el 20 de septiembre de 2019)

International Telecommunication Union. Global Cybersecurity Index (GCI) 2017. 19 de julio de 2017. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-R1-PDF-E.pdf (Consultado el 24 de septiembre de 2019)

International Telecommunication Union. Global Cybersecurity Index (GCI) 2018. https://www.itu.int/en/ITU-D/Cybersecurity/Documents/draft-18-00706_Global-Cybersecurity-Index-EV5_print_2.pdf (Consultado el 24 de septiembre de 2019)

Johnson, Keith y Groll, Elias. The Improbable Rise of Huawei. Foreign Policy. Abril 3, 2019. https://foreignpolicy.com/2019/04/03/the-improbable-rise-of-huawei-5g-global-network-china/ (Consultado el 30 de agosto de 2019)

Kania, E, Sacks, S, Triolo, P y Webster, G. 2017. China's Strategic Thinking on Building Power in Cyberspace. https://www.newamerica.org/cybersecurity-initiative/blog/chinas-strategic-thinking-building-power-cyberspace/ (Consultado el 28 de agosto de 2019)

Keohane, Robert O., and Joseph S. Nye. 1977. *Power and interdependence: world politics in transition*. Boston: Little, Brown.

King, I, Bergen, M, y Brody, B. 2019. Top U.S. Tech Companies Begin to Cut Off Vital Huawei Supplies. *Bloomberg*, 19 de mayo de 2019. https://www.bloomberg.com/news/articles/2019-05-19/google-to-end-some-huawei-business-ties-after-trump-crackdown (Consultado el 4 de septiembre de 2019)

Kobayashi, Shigeo, Jia Baobo, y Junya Sano. 1999. "Three Reforms in China: Progress and Outlook". https://bit.ly/2PBVPxB (Consultado el 1 de mayo de 2019).

Kuo, Lily. 2019. Chinese surveillance company tracking 2.5m Xinjiang residents. The Guardian, Febrero 18 de 2019. https://www.theguardian.com/world/2019/feb/18/chinese-surveillance-company-tracking-25m-xinjiang-residents (Consultado el 30 de agosto de 2019)

Levy, Irene. 2019. Satélites vs. 5G. El Universal, 3 de junio de 2019. https://www.eluniversal.com.mx/columna/irene-levy/cartera/satelites-vs-5g (Consultado el 12 de septiembre de 2019)

Lian, Yi-Zheng. 2019. Where Spying Is the Law. *The New York Times*. Marzo 13, 2019. https://www.nytimes.com/2019/03/13/opinion/china-canada-huawei-spying-espionage-5g.html (Consultado el 12 de septiembre de 2019).

Luo, Yan. 2013. Building World-Class Universities in China en *Institutionalization of World-Class University in Global Competition*. Cheol y Kehm (editores) Springer, 2013.

MacEnchroe, T y Kroupa J. 2019. Former Huawei employees say client information was discussed at Chinese Embassy. *Radio Prague International*, 22 de julio de 2019. https://www.radio.cz/en/section/curraffrs/former-huawei-employees-say-client-information-was-discussed-at-chinese-embassy (Consultado el 29 de agosto de 2019)

Manheimer Swartling. 2019. Applicability of Chinese National Intelligence Law to Chinese and non-Chinese Entities. Enero de 2019. https://www.mannheimerswartling.se/globalassets/nyhetsbrev/msa_nyhetsbrev_national-intelligence-law_jan-19.pdf (Consultado el 2 de septiembre de 2019)

Mazarr, Michael J. 2019. "This is Not a Great Power-Competition". Foreign Afairs, https://fam.ag/2ZHpl4D (Consultado el 29 de mayo de 2019).

McGrattan, Ellen R. 2016. “China’s Foreign Investment”..https://bit.ly/2HFSPJU (Consultado el 1 de mayo de 2019).

Micheli, Jordy y Carrillo, Jorge. The globalization strategy of a chinese multinational: Huawei in Mexico. Frontera Norte, Vol. 28, Núm. 56, Julio-Diciembre de 2016, Pp. 35-58. http://www.scielo.org.mx/pdf/fn/v28n56/0187-7372-fn-28-56-00035.pdf (Consultado el 3 de septiembre de 2019)

Minister of Communications and The Arts. 2018. Government Provides 5G Security Guidance To Australian Carriers. https://www.minister.communications.gov.au/minister/mitch-fifield/news/government-provides-5g-security-guidance-australian-carriers (Consultado el 12 de septiembre de 2019)

NASA. 2018. 2019. What is a relay satellite? https://www.nasa.gov/directorates/heo/scan/communications/outreach/funfacts/txt_relay_satellite.html (Consultado el 12 de septiembre de 2018)

OCDE. 2019, Gross domestic spending on R&D (indicator). doi: 10.1787/d8b068b4-en (Consultado el 13 de Agosto de 2019)

Office of the United States Trade Representative Executive Office Of The President. 2018. Findings of The Investigation Into China’s Acts, Policies, and Practices Related to Technology Transfer, Intellectual Property, and Innovation Under Section 301 of the Trade Act Of 1974. https://ustr.gov/sites/default/files/Section%20301%20FINAL.PDF Marzo 22, 2018. (Consultado el 12 de septiembre de 2019).

Okoshi. Yuki. 2019. China's research papers lead the world in cutting-edge tech. Enero 6, 2019. *Nikkei Asian Review*. https://asia.nikkei.com/Business/China-tech/China-s-research-papers-lead-the-world-in-cutting-edge-tech (Consultado el 19 de agosto de 2019)

Osborne, H, y Cutler, S. 2019. Chinese border guards put secret surveillance app on tourists' phones. *The Guardian*, Julio 2 de 2019. https://www.theguardian.com/world/2019/jul/02/chinese-border-guards-surveillance-app-tourists-phones (Consultado el 26 de agosto de 2019)

Parkinson, Joe, Nicholas Bariyo and Josh Chin. 2019. “Huawei Technicians Helped African Governments Spy on Political Opponents”. *The Wall Street Journal*. https://www.wsj.com/articles/huawei-technicians-helped-african-governments-spy-on-political-opponents-11565793017 (Consultado el 9 de septiembre de 2019).

Sacks, Samm. 2019. China’s Privacy Conundrum, Febrero 14 del 2019. https://www.newamerica.org/weekly/edition-236/chinas-privacy-conundrum/ (Consultado el 30 de agosto de 2019)

Sacks, Samm. 2019. On “China: Challenges to U.S. Commerce” A Hearing Before the Senate Committee on Commerce, Science, and Transportation’s Subcommittee on Security. Marzo 7 de 2019. https://www.commerce.senate.gov/public/_cache/files/7109ed0e-7d00-

4ddc-998e-b99b2d19449a/C71FB6E4FAB0FF56FD3E8BBC1B9E68A4.03-07-2019-sacks-testimony.pdf (Consultado el 3 de septiembre de 2019)

Sacks, Samm. 2019. Samm Sacks Testifies Before House Foreign Affairs Committee on 'Smart Competition' With China. Mayo 10 de 2019, *New America.* https://www.newamerica.org/cybersecurity-initiative/digichina/blog/samm-sacks-testifies-house-foreign-affairs-committee-smart-competition-china/ (Consultado el 4 de septiembre de 2019)

Schake, Kori. 2018. "Beijing's Cravings, Kremlin's Gremlins: Freedom's Foes". *Halifax Papers 2018* Halifax International Security Forum.

Sheehan, Mat. 2018. Trump's Trade War Isn't About Trade, It's About Technology. Macro Polo, abril 3 de 2018. https://macropolo.org/analysis/trumps-trade-war-isnt-about-trade-its-about-technology/ (Consultado el 3 de septiembre de 2019)

South China Morning Post. 2018. Tech giant Huawei banned from New Zealand's 5G network over 'significant' security risks. 28 de noviembre de 2018. https://www.scmp.com/news/asia/australasia/article/2175374/tech-giant-huawei-banned-new-zealands-5g-network-over (Consultado el 5 de septiembre de 2019)

Statista. 2016. Market share held by Huawei in the mobile phone market in Mexico in 2014 and 2016. https://www.statista.com/statistics/728173/huawei-market-share-mexico/ (Consultado el 23 de septiembre de 2019)

Stratfor. 2019. "Trump Looks to Open Another Front in The Trade War with China." *Stratf*or,.https://bit.ly/2MOP7C0 (Consultado el 27 de agosto de 2019)

Tao, Li. 2019. Japan latest country to exclude Huawei, ZTE from 5G roll-out over security concerns. *South China Morning Post*, 10 de diciembre de 2018. https://www.scmp.com/tech/tech-leaders-and-founders/article/2177194/japan-decides-exclude-huawei-zte-government (Consultado el 5 de septiembre de 2019)

Tao, T, Cremer D, y Chunbo W. 2018. Huawei, liderazgo cultura y conectividad. Ed. LID, 2018.

The Economist. 2019. A new kind of cold war. Mayo 16, 2019. Disponible en: https://www.economist.com/leaders/2019/05/16/a-new-kind-of-cold-war?cid1=cust/ednew/n/bl/n/2019/05/16n/owned/n/n/nwl/n/n/la/240955/n (Consultado el 18 de agosto de 2019)

The Economist. 2018. China is seeking to become a "cyber-superpower", Marzo 20, 2018. https://www.economist.com/graphic-detail/2018/03/20/china-is-seeking-to-become-a-cyber-superpower (Consultado el 27 de agosto de 2019)

The Economist. 2019. Huawei is at the centre of political controversy. Abril 27, 2019. Disponible en: https://www.economist.com/briefing/2019/04/27/huawei-is-at-the-centre-of-political-controversy

The Guardian. 2019. May to ban Huawei from providing 'core' parts of UK 5G network. 24 de abril de 2019. https://www.theguardian.com/technology/2019/apr/24/may-to-ban-huawei-from-supplying-core-parts-of-uk-5g-network (Consultado el 4 de septiembre de 2019)

The Guardian. 2019. Poland arrests Huawei worker on allegations of spying for China. Enero 11 de 2019. https://www.theguardian.com/technology/2019/jan/11/huawei-employee-arrested-in-poland-over-chinese-spy-allegations (Consultado el 30 de agostro de 2019)

Triolo, Paul. 2019. US-China trade: What's up with Huawei? *Eurasia Live*. 21 de mayo de 2019. https://www.eurasiagroup.net/live-post/us-china-trade-whats-up-with-huawei (consultado el 22 de agosto de 2019)

United States Census Bureau. 2019. "Trade in Goods with China". https://bit.ly/1BpSO1N (Consultado el 1 de mayo de 2019).

Weber, Jonathan. Explainer: What is China's Huawei Technologies and why is it controversial? Reuters. Diciembre 6, 2018. https://www.reuters.com/article/us-usa-china-huawei-explainer/explainer-what-is-chinas-huawei-technologies-and-why-is-it-controversial-idUSKBN1O5172 (Consultado el 4 de septiembre de 2019)

Westad, Odd Arne. 2019. "The Sources of Chinese Conduct". Foreign Affairs, Septiembre/octubre, 2019. https://fam.ag/2yVSzBV (Consultado el 12 de septiembre de 2019).

Wolfe, Henry. 2019. Australia Should Reverse Its Huawei 5G Ban. The New York Times. https://www.nytimes.com/paidpost/huawei/australia-should-reverse-its-huawei-5g-ban.html (Consultado el 5 de septiembre de 2019)

Xinhuanet. 2019. "The five fallacies in Pence's China speech". https://bit.ly/2zGTV3J (Consultado el 12 de septiembre de 2019).

Xu, Jodi. 2019. Could US' Huawei worries be solved with global cybersecurity plan? *South China Morning Post*, 6 de agosto de 2019. https://www.scmp.com/news/china/article/3021511/could-us-huawei-worries-be-solved-global-cybersecurity-plan (Consultado el 6 de septiembre de 2019).

Zhou, Christina Y Xiao, Bang. 2018. "China's 40 years of economic reform that opened the country up and turned it into a superpower". ABC News, 1 de diciembre de 2018. https://ab.co/2ITp0bb (Consultado el 12 de septiembre de 2019).