SEGURIDAD Y DEFENSA
ICP POLICY LAB

Entendiendo el riesgo de las empresas chinas de tecnologías de la información y comunicación (TIC)

LA PERSPECTIVA DE LA **REPÚBLICA CHECA**

2023

ICP
DESDE 1987

SINOPSIS
CHINA IN CONTEXT AND PERSPECTIVE

Entendiendo el riesgo de las empresas chinas de tecnologías de la información y comunicación (TIC)

Autores
Proyecto Sinopsis
Praga
República Checa

Sinopsis es un proyecto con sede en la República Checa implementado por la asociación sin ánimo de lucro AcaMedia z.ú., en colaboración académica con el Departamento de Sinología de la Universidad Carolina en Praga. Su objetivo es ofrecer un panorama regular de los acontecimientos en China y sus impactos en el mundo exterior desde las perspectivas de observadores checos, chinos e internacionales. https://sinopsis.cz/en/

Traducción y divulgación
Instituto de Ciencia Política Hernán Echavarría Olózaga – ICP -

El ICP es un centro de pensamiento de origen empresarial, apartidista, privado e independiente. Desde 1987 defiende las libertades económicas y las instituciones de la democracia liberal.

Instituto de Ciencia Política Hernán Echavarría Olózaga - ICP
Calle 70 #7a - 29
(+57) 313 431 20 95
www.icpcolombia.org

Diciembre 2023
Bogotá, Colombia

Contenido

Resumen ejecutivo

- Las empresas chinas de Tecnologías de la Información y la Comunicación -TIC- mantienen conexiones extensas y permanentes con el gobierno chino y el Partido Comunista Chino (PCCh), incluyendo sus servicios de inteligencia, agencias de seguridad y el ejército.

- El marco legal en la República Popular China (RPC) obliga a las empresas chinas de TIC a participar activamente en actividades de inteligencia. A cambio, el gobierno chino promete protección para individuos y entidades involucradas en tales actividades. La estructura política de la RPC no permite a las empresas chinas de TIC rechazar la cooperación con las autoridades estatales.

- La Ley de Inteligencia del Estado es la ley más importante de las normas de seguridad estatal en cuanto define las obligaciones de individuos y organizaciones para participar en actividades de inteligencia estatal.

- El PCCh controla estrictamente las operaciones de las empresas privadas a través de la presencia legalmente requerida de células del partido en las estructuras de las empresas.

- La inclusión de productos de empresas chinas de TIC en sistemas gubernamentales cruciales y en Infraestructuras Críticas de Información (ICI) representa un riesgo excepcionalmente alto. Descuidar estos riesgos podría resultar en impactos adversos significativos en la seguridad nacional de un país determinado.

- Un proveedor chino que actúe en nombre o facilite la actividad del aparato de seguridad estatal chino puede representar una amenaza para la confidencialidad, integridad y disponibilidad de las redes 5G.

- Medidas de seguridad como pruebas y certificaciones no ofrecen garantías adecuadas en ausencia de confianza en el proveedor.

- **El enfoque de la República Checa ha contribuido a establecer los aspectos no técnicos de la ciberseguridad como igualmente importantes, impulsando la evaluación de riesgos basada en la confianza como un enfoque central en la seguridad de las redes 5G**.

Presentación

En el marco del trabajo que desarrolla el Instituto de Ciencia Política Hernán Echavarría Olózaga, a través del ICP Policy Lab en Seguridad y Defensa, para generar conocimiento sobre las dinámicas geopolíticas y los riesgos que surgen para Colombia frente a la penetración e injerencia de regímenes autocráticos, solicitó la colaboración del Proyecto Sinopsis de República Checa, con el fin de dar a conocer la experiencia de ese país con los proveedores chinos de tecnología para las redes móviles de quinta generación 5G.

El presente documento complementa la publicación del ICP sobre **"La tecnología 5G china y los riesgos para Colombia: Análisis comparado y recomendaciones de política".**

Con la traducción y publicación del presente reporte elaborado por el Proyecto Sinopsis, debidamente soportado y documentado, desde el ICP se busca sensibilizar a la opinión pública y los tomadores de decisión en Colombia, sobre la importancia de adoptar medidas para enfrentar los riesgos que surgen al permitir que en el sector de las Tecnologías de la Información y la Comunicación -TIC- participen empresas chinas que han sido cuestionadas e incluso excluidas o restringidas en varios países.

Por tratarse de un sector estratégico y crítico para el futuro del país, es necesario reconocer las razones por las que en varios países no se les permite participar como proveedores.

En el caso europeo, tanto a nivel nacional como comunitario, se han adoptado estas medidas debido a que por mandato de la legislación de la República Popular China (RPC) los ciudadanos y las empresas deben entregar información y permitir el acceso de los servicios de seguridad e inteligencia del Estado chino, así como la incidencia del Partido Comunista Chino (PCCh) en las empresas públicas y privadas. Lo que plantea cuestionamientos frente a los riesgos que surgen por las posibles "puertas traseras" que darían acceso al gobierno chino a la información y los datos, tanto de las personas, el sector empresarial y el gobierno.

Como concluye el presente documento, resulta fundamental reconocer que, aunque las empresas chinas presentan soluciones tecnológicas avanzadas y competitivas, la realidad es que el contexto político y legal en el que están obligadas y dispuestas a operar plantea dudas sobre la confiabilidad para salvaguardar el futuro del sector TIC y garantizar la integridad de la información y los datos. Ignorar incluso los riesgos más elementales asociados con las relaciones de Huawei con el partido-estado chino podría acarrear graves implicaciones para la seguridad nacional.

Carlos Augusto Chacón Monsalve
Director ejecutivo
Instituto de Ciencia Política Hernán Echavarría Olózaga

Entendiendo el riesgo de las empresas chinas de tecnologías de la información y comunicación (TIC): La perspectiva de la República Checa

Empresas chinas de TIC y el Estado-Partido chino

En las últimas dos décadas, las empresas chinas de tecnologías de la información y comunicación (TIC) se han posicionado como actores clave a nivel global, especialmente en la investigación y desarrollo de tecnologías innovadoras. Su éxito se atribuye a un vasto conjunto de talentos y sustanciales inversiones en investigación y desarrollo. Otro factor es el considerable respaldo del gobierno, que implica subsidios importantes e instancias de espionaje industrial en las que el gobierno chino brindó asistencia tanto a empresas estatales como privadas.

El contexto político y legal dentro de la República Popular China (RPC) emerge como un problema prominente y crítico cuando se suma a las conexiones organizativas y personales de las empresas chinas de TIC con los intereses del Partido Comunista Chino (PCCh). Leyes como la Ley de Inteligencia del Estado, la Ley de Empresas, o la Ley de Seguridad Cibernética, junto con el marco político en China, esencialmente no permiten que las empresas chinas de TIC rechacen la cooperación en las actividades de espionaje y vigilancia de la (RPC) y al mismo tiempo incentivan fuertemente dicha cooperación.

Aunque muchas empresas chinas de TIC pueden considerarse oficialmente entidades privadas, para operar deben ajustarse a las regulaciones establecidas. Las adquisiciones de Anbang Insurance[1] y CEFC[2] subrayan esta realidad. La compra por parte del gobierno chino de participaciones mayoritarias en empresas como Tencent o Alibaba[3] demuestra que el Estado chino está dispuesto a asumir el control de empresas privadas que caen en desgracia con el liderazgo del Partido Comunista Chino (PCCh). El escenario hipotético de que Huawei o ZTE rechacen la solicitud del gobierno chino de participar en actividades de inteligencia probablemente resultaría en una toma directa de la empresa por parte del Estado, acompañada de severas sanciones para sus directivos.

Las relaciones dinámicas entre el PCCh, el Estado y tanto las empresas estatales como privadas van más allá de la mera intimidación. Las empresas chinas de TIC han estado activamente involucradas en la investigación y desarrollo de tecnología con

[1] China seizes control of Anbang Insurance as chairman prosecuted, https://www.reuters.com/article/us-china-anbang-regulation-idUSKCN1G7076/
[2] State-owned Citic takes over troubled tycoon Ye Jianming's investments in Czech Republic, https://www.scmp.com/business/companies/article/2142579/state-owned-citic-takes-over-troubled-tycoon-ye-jianmings
[3] China to take 'golden shares' in tech firms Alibaba and Tencent, https://www.theguardian.com/world/2023/jan/13/china-to-take-golden-shares-in-tech-firms-alibaba-and-tencent

aplicaciones militares o de seguridad interna desde su inicio. Estas empresas también reconocen que se beneficiarán del apoyo del gobierno, independientemente de las posibles repercusiones, como daños a su reputación en el extranjero debido a fallas percibidas o reales en la protección de la información del cliente. Además, generalmente pueden contar con el principio de negación plausible, lo que dificulta demostrar de manera concluyente cualquier intención maliciosa por parte de las empresas chinas de TIC.

La formación de afiliaciones directas o indirectas entre empresas de TIC y los servicios de inteligencia, agencias de seguridad del Estado y el ejército de la RPC se fomenta aún más a través de la investigación y desarrollo orientado militarmente bajo el paraguas de la Fusión Militar-Civil (FMC)[4]. Un informe de 2012, encargado por la Comisión de Revisión Económica y de Seguridad entre Estados Unidos y China (USCC), proporciona una visión integral de los proyectos del Ejército de Liberación Popular (PLA) que involucraban a Huawei y ZTE en ese momento[5]. Dado la tendencia continua de integrar los sectores civil y militar, es probable que la participación de las empresas de TIC en la investigación militar se haya expandido aún más desde la publicación del informe hace una década.

Obligación de Cooperar

Las autoridades chinas adoptan una definición integral de la seguridad estatal, alejándose del entendimiento convencional de la seguridad nacional predominante en la región euroatlántica.

Una característica distintiva del enfoque chino hacia la seguridad estatal es la expectativa de que cada ciudadano y organización contribuya activamente a la seguridad estatal, según lo dictan las leyes de la RPC. El objetivo principal de obligar legalmente a los individuos a garantizar la seguridad estatal es mantener la continuidad del dominio del PCCh.

La interconexión entre el Estado y el PCCh es absoluta y, en gran medida, más estrecha que la observada en los regímenes comunistas del Bloque del Este. La influencia del PCCh sobre las instituciones estatales de la RPC ha sido siempre notoria. Sin embargo, bajo el liderazgo actual del Presidente del Partido Comunista, Xi Jinping, el control ejercido por los órganos del partido se ha fortalecido aún más. Numerosas instituciones estatales que antes estaban bajo la jurisdicción del Consejo de Estado de la República Popular China (Gobierno de la RPC) ahora están directamente bajo el control del Comité Central del PCCh. Por ejemplo, la Administración del Ciberespacio de China fue transferida del Consejo de Estado a órganos del partido en 2014, y en 2018, el Comité

[4] The foundation of innovation under military-civil fusion: The role of universities, https://sinopsis.cz/en/mcf/
[5] Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage, https://www.uscc.gov/Research/occupying-information-high-ground-chinese-capabilities-computer-network-operations-and. USCC is a commission created and funded by the US Congress to research and monitor US-China security and economic issues.

Central del Ciberespacio del Consejo Central del PPCh asumió la autoridad superior sobre la agencia de ciberseguridad de China[6].

Un factor que contribuye al perfil de riesgo de las empresas chinas es la falta de independencia genuina en el poder judicial de la RPC, dejando escasas opciones para las empresas chinas que buscan protección legal contra las demandas de las autoridades estatales. Los tribunales de la RPC están obligados a considerar las directrices del PCCh y, simultáneamente, están sujetos a la supervisión de la fiscalía y las asambleas populares (siendo el Congreso Nacional del Pueblo el nivel más alto de las asambleas populares). Un factor significativo es el considerable riesgo personal que asumirían los líderes empresariales chinos si desafiaran a las autoridades estatales (y, por ende, al liderazgo del PCCh) en los tribunales. Sin embargo, tal escenario sigue siendo en gran medida teórico, ya que es muy poco probable que alguna organización o individuo considere recurrir al sistema judicial para impugnar al gobierno en asuntos relacionados con la seguridad estatal.

La Advertencia de 2018 y Huawei en la República Checa

El 17 de diciembre de 2018, la Agencia Nacional de Ciberseguridad e Información (NUKIB) de la **República Checa emitió la primera advertencia regulatoria[7] de Europa contra el uso de tecnología de las empresas chinas Huawei y ZTE**. En el cuarto punto de la justificación detrás de la advertencia, NUKIB destacó el entorno legal y político de la RPC, enfatizando que las empresas chinas están obligadas a cooperar en el avance de los intereses de la RPC:

> *El entorno legal y político de la República Popular China ("RPC") en el cual operan principalmente las empresas y cuyas leyes deben cumplir, exige a las empresas privadas cooperar para satisfacer los intereses de la RPC, incluida la participación en actividades de inteligencia, etc. Al mismo tiempo, estas empresas generalmente no se abstienen de tal cooperación con el Estado; en este entorno, los esfuerzos para proteger los intereses de los clientes a expensas de los intereses de la RPC se reducen significativamente. Según la información disponible, existe un vínculo organizativo y personal entre estas empresas y el Estado. Por lo tanto, esto suscita preocupaciones de que los intereses de la RPC pueden priorizarse sobre los intereses de los usuarios de las tecnologías de estas empresas.*

La preocupación de NUKIB no solo se centraba en la confidencialidad de los datos, sino también en su integridad y, más importante aún en el caso de las redes de telecomunicaciones, la disponibilidad de las futuras redes 5G. NUKIB sigue preocupada

[6] Behind the Facade of China's Cyber Super-Regulator, https://digichina.stanford.edu/work/behind-the-facade-of-chinas-cyber-super-regulator/
[7] SOFTWARE AND HARDWARE OF HUAWEI AND ZTE IS A SECURITY THREAT, https://www.govcert.cz/en/info/events/2682-software-and-hardware-of-huawei-and-zte-is-a-security-threat/

de que Huawei o ZTE, bajo la influencia de las instituciones de seguridad del Estado chino, puedan desactivar elementos clave de la infraestructura de información crítica de la República Checa.

En el momento de la advertencia de NUKIB, Huawei había establecido una presencia significativa en la República Checa, especialmente a través de su participación en la infraestructura de los tres principales operadores móviles del país: O2, Vodafone y T-Mobile.

Un factor clave que impulsó un examen más cercano por parte de la comunidad de seguridad checa sobre las actividades de Huawei fue una oferta pública para construir un centro de datos para la empresa energética estatal CEZ. Al igual que los operadores móviles, CEZ es reconocida como una entidad de infraestructura de información crítica y está sujeta a la jurisdicción regulatoria de NUKIB. En el caso de la oferta del centro de datos, las tres ofertas más bajas provinieron de empresas que eran socias locales de Huawei[8].

Los críticos de la licitación argumentaron en ese momento que el único criterio considerado fue el precio de la oferta, señalando que las ofertas de los socios de Huawei eran excepcionalmente bajas, **generando preocupaciones sobre su viabilidad sin posibles subsidios de la empresa china.** Esto ha llevado a especulaciones de que los motivos de Huawei pueden no haber sido únicamente comerciales. Como en muchos países, la ley de licitación pública en la República Checa fomenta la selección de ofertas con la oferta más baja para incentivar el ahorro de dinero de los contribuyentes.

La ley incluye disposiciones de seguridad nacional, pero rara vez se invoca para evitar una revisión adicional del organismo encargado de vigilar la libre competencia. Esto es, por supuesto, un comportamiento problemático en el caso de una agencia u organización de licitación donde las consideraciones de seguridad nacional son apropiadas y razonables, y el valor financiero de la oferta no debería ser el único factor determinante. La comunidad de inteligencia de la República Checa planteó el problema en 2017; **en particular, la agencia de contrainteligencia del país, BIS, señaló en su informe anual que las empresas chinas no tienen dificultades para cumplir con los requisitos de seguridad formales para participar en licitaciones, a pesar de estar asociadas con riesgos de seguridad derivados de los fuertes vínculos entre estas empresas y el Estado chino y sus intereses en política exterior[9].**

La advertencia de NUKIB no prohibió la tecnología de Huawei y ZTE. Sin embargo, **elevó el nivel de amenaza al máximo para la evaluación obligatoria de riesgos para las entidades bajo la Ley de Ciberseguridad Checa (CSA).** Esa ley requería que las organizaciones que desearan adquirir nuevos equipos de tecnologías TIC implementaran costosas medidas de protección si elegían a Huawei o ZTE, o si optaban

[8] China's Huawei wants to get into ČEZ, it offered the best price of data centre equipment, https://www.lupa.cz/clanky/cinsky-huawei-se-chce-dostat-do-cezu-nabidl-nejnizsi-ceny-na-vybaveni-datacentra/

[9] Security Information Service Annual Report 2016, https://www.bis.cz/vyrocni-zprava16e1.html?ArticleID=1136

por otro proveedor. **La advertencia incentivó las consideraciones de seguridad nacional al hacer que la oferta a menudo más barata de Huawei fuera potencialmente más cara que la de sus competidores debido a la necesidad de comprar soluciones tecnológicas adicionales cuyo único propósito era monitorear el funcionamiento del equipo de Huawei.**

Sin embargo, aunque la advertencia cumplió su propósito, se necesita una solución más permanente. Actualmente, después de un período de solicitud de comentarios públicos y una revisión obligatoria por parte de otras agencias gubernamentales, una enmienda a la CSA busca establecer un mecanismo que permita la prohibición de proveedores no confiables y de alto riesgo. **En 2022, NUKIB, en cooperación con los servicios de inteligencia y las agencias gubernamentales relevantes, emitió "La Recomendación para evaluar la confiabilidad de los proveedores de tecnología de redes 5G en la República Checa"[10] que delineaba las prioridades clave de la comunidad[11] de seguridad nacional de la República Checa en la selección de proveedores para infraestructuras de información crítica como las redes 5G, a saber, que el proveedor debe provenir de un país con un gobierno democráticamente elegido, un poder judicial independiente y que no participe en actividades contrarias a los intereses de la República Checa o de sus aliados.**

Leyes chinas relevantes para la Advertencia de NUKIB en 2018 contra Huawei y ZTE

Ley de Seguridad del Estado (2015)

La RPC revisó su legislación de seguridad del Estado entre 2014 y 2017, introduciendo la Ley de Seguridad del Estado (国家安全法) en julio de 2015. Los Artículos 4 y 15 reconocen explícitamente el papel de liderazgo del PCCh en asuntos de seguridad del Estado.

El Artículo 77 delinea las responsabilidades de ciudadanos y organizaciones con respecto a la seguridad del Estado:

1. Cumplir con las disposiciones pertinentes de la Constitución, leyes y regulaciones relacionadas con la seguridad nacional.
2. Informar de manera oportuna sobre actividades que representen una amenaza para la seguridad nacional.
3. Proporcionar verazmente pruebas relacionadas con actividades que pongan en peligro la seguridad nacional.

[10] The Recommendation for assessing the trustworthiness of technology suppliers of 5G networks in the Czech Republic, https://www.nukib.cz/en/infoservis-en/news/1805-the-recommendation-for-assessing-the-trustworthiness-of-technology-suppliers-of-5g-networks-in-the-czech-republic/
[11] Loosely defined as organizations tasked with protection of national security like intelligence agencies, national policy, NUKIB, and ministries of interior, defence, and foreign affairs.

4. Ofrecer condiciones para facilitar los esfuerzos de seguridad nacional y brindar otras formas de asistencia.
5. Suministrar el apoyo y la asistencia necesarios a los órganos de seguridad pública, los órganos de seguridad del estado o los órganos militares pertinentes.
6. Salvaguardar la confidencialidad de los secretos de estado de los que tengan conocimiento.
7. Cumplir con otros deberes estipulados por la ley o regulaciones administrativas.

La Ley de Seguridad del Estado establece una obligación general para ciudadanos y organizaciones de asistir a las autoridades estatales en asuntos de seguridad del Estado. Leyes subsecuentes amplían esta obligación definida de manera amplia, adaptándola a las actividades específicas delineadas en cada ley respectiva.

Ley de Inteligencia del Estado (2017)

La Ley de Inteligencia del Estado es la ley más importante de la colección de actos de seguridad del Estado en términos de definir las obligaciones de individuos y organizaciones para participar en actividades de inteligencia del Estado. El Artículo 7 define la obligación de entidades y su protección por parte del Estado:

> *Todas las organizaciones y ciudadanos están obligados por ley a apoyar el trabajo nacional de inteligencia, cooperar y mantener en secreto los secretos que aprendan en relación con el trabajo nacional de inteligencia.*
>
> *El Estado protege a individuos y organizaciones que contribuyen al apoyo y la cooperación en el contexto del trabajo nacional de inteligencia.*

El Artículo 14 de la ley enfatiza que las instituciones estatales relevantes tienen derecho a exigir la cooperación de individuos y organizaciones:

> *Los servicios de inteligencia nacionales pueden, de acuerdo con las regulaciones estatales relacionadas, solicitar a las autoridades competentes, organizaciones y ciudadanos que proporcionen el apoyo y la cooperación necesarios.*

Por razones obvias, la ley no menciona la inteligencia extranjera, pero se conocen casos de participación de empresas privadas en actividades de inteligencia[12].

[12] For example: U.S. Charges Three Chinese Hackers Who Work at Internet Security Firm for Hacking Three Corporations for Commercial Advantage, https://www.justice.gov/opa/pr/us-charges-three-chinese-hackers-who-work-internet-security-firm-hacking-three-corporations

Ley de Empresas (2013)

A diferencia de las leyes mencionadas anteriormente, esta regulación no se refiere directamente a la seguridad del Estado. Sin embargo, el Artículo 19 introduce un mecanismo para la influencia del PCCh en las empresas:

> *Dentro de la empresa se establecerá una organización del Partido Comunista de China para llevar a cabo actividades del partido de acuerdo con la Constitución del Partido Comunista de China. La empresa está obligada a facilitar las condiciones necesarias para el funcionamiento de la organización del partido.*

La obligación de establecer una célula del partido no es un desarrollo reciente. Después de la asunción de Xi Jinping al liderazgo tanto del Partido como del Estado, esta regla se ha aplicado de manera más rigurosa, con frecuencia el PCCh ocupando posiciones en los niveles más altos de empresas aparentemente privadas. En relación con la obligación de ciudadanos y organizaciones en la RPC de participar en actividades de inteligencia, derivada de la amplia interpretación de la obligación de garantizar la seguridad del Estado, es crucial examinar los mecanismos a través de los cuales el PCCh influye en empresas nominalmente privadas, como Huawei o ZTE.

Según información de fuentes abiertas, ya en 2007, cuando la presencia de células del partido no era estrictamente obligatoria en empresas nominalmente privadas, Huawei tenía 56 células principales del partido y 300 células de nivel inferior que involucraban a 12,000 empleados. El actual líder de la organización del partido en Huawei, Zhou Daiqi (周代琪), también ocupa el cargo de Vicepresidente Senior de Huawei, representando a la empresa en el nivel más alto.

Inspiración australiana

Si bien la advertencia de la República Checa fue la primera vez que un Estado miembro de la UE tomó medidas regulatorias contra empresas chinas de TIC, el enfoque que tomaron las autoridades checas se puede rastrear hasta la decisión australiana de prohibir a Huawei y ZTE en las redes 5G apenas tres meses antes. A finales de agosto de 2018, el gobierno australiano tomó la decisión de excluir a Huawei y ZTE de futuros proyectos de desarrollo de redes 5G. Aunque la decisión del gobierno no nombra específicamente a Huawei o ZTE, establece en la parte clave[13]:

> *El Gobierno considera que la participación de proveedores que probablemente estén sujetos a direcciones extrajudiciales de un gobierno extranjero que entren en conflicto con la ley australiana, puede suponer un riesgo de que el operador no proteja adecuadamente una red 5G contra el acceso o la interferencia no autorizados.*

[13] 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

Esto constituye una clara referencia a las disposiciones delineadas en los Artículos 7 y 14 de la Ley de Inteligencia del Estado de China. Aunque Canberra no especificó explícitamente las empresas chinas de TIC en su decisión, es evidente que Huawei y ZTE cumplen con los criterios. El gobierno australiano puede invocar las Reformas de Seguridad del Sector de las Telecomunicaciones (TSSR, por sus siglas en inglés) como base legal para su determinación.

Otro argumento presentado por las autoridades australianas sostiene que, a diferencia de las generaciones anteriores de redes, las redes 5G carecen de una distinción clara entre componentes centrales y periféricos[14].

Esencialmente, el gobierno australiano argumentó que en las redes 5G, es impráctico mitigar los riesgos al restringir a empresas problemáticas solo de los sistemas centrales. Aseguran que, a diferencia de las redes existentes 4G/LTE (y anteriores), la red 5G no puede segmentarse en un núcleo donde se prohíben los proveedores problemáticos y una red de acceso donde pueden operar.

Inadecuación de Salvaguardias Técnicas: de la advertencia a medidas estratégicas

Una de las contribuciones más significativas de la advertencia de NUKIB es que elevó la confianza, o la falta de ella, en el proveedor a un nivel que antes estaba dominado por medidas técnicas para asegurar una red de telecomunicaciones.

En mayo de 2019, NUKIB convocó la primera Conferencia de Seguridad 5G de Praga, que resultó en una serie de recomendaciones conocidas como Propuestas de Praga (PP). Sobre el papel de las medidas no técnicas, las PP afirmaron:

> *La ciberseguridad no puede considerarse como un problema puramente técnico. Una infraestructura segura, protegida y resistente requiere estrategias nacionales adecuadas, políticas sólidas, un marco legal integral y personal dedicado, capacitado y educado de manera apropiada. Una ciberseguridad sólida respalda la protección de las libertades civiles y la privacidad.*
>
> *Al enfrentarse a amenazas de ciberseguridad, no solo debe tenerse en cuenta su naturaleza técnica, sino también el comportamiento específico de actores malintencionados que buscan explotar nuestra dependencia de las tecnologías de comunicación.*

El énfasis en los aspectos no técnicos de la ciberseguridad también surgió de la falta de confianza en la adecuación de las soluciones técnicas conocidas. Se propuso probar equipos en centros especializados para dispositivos de red, seguido de la certificación, como estrategia para mitigar los riesgos de seguridad durante su operación. Huawei

[14] Ibidem.

ofreció sus instalaciones para pruebas y en 2019 inauguró un "Centro de Transparencia de Ciberseguridad de Huawei" en Bruselas[15].

Por lo general, **los componentes de red se someten a pruebas antes de su implementación. Sin embargo, estos dispositivos no son impermeables a los cambios, y cada uno se actualiza continuamente por diversas razones después de la fase de prueba inicial.** Una actualización de firmware puede corregir una vulnerabilidad o potencialmente introducir una nueva. Este principio generalmente es válido para el equipo de cualquier fabricante. La complejidad se intensifica para las empresas de tecnologías de la información y la comunicación (TIC) con obligaciones legales de actuar en interés del gobierno de su país de origen, amplificando significativamente el potencial para el uso indebido de sus tecnologías más allá de los riesgos estándar asociados con las TIC. Estas limitaciones socavan seriamente la efectividad de los centros de pruebas. Las deficiencias más críticas son:

- Los centros de pruebas proporcionan una capacidad altamente restringida para monitorear y mitigar los riesgos asociados con la implementación de tecnologías de información y comunicación (TIC). **El principal desafío radica en la imposibilidad práctica de garantizar que el equipo sometido a pruebas permanezca no perjudicial después de las actualizaciones de software y hardware.**
- Cuando los centros de pruebas son establecidos por proveedores (por ejemplo, Huawei) sin supervisión independiente, el nivel de transparencia depende completamente de la disposición de estas empresas.
- La prueba de productos es excepcionalmente demorada. Los códigos fuente de los dispositivos pueden ser sumamente extensos, y los propios dispositivos comprenden numerosos componentes y circuitos electrónicos con funciones diversas. Basta con que un componente de un dispositivo específico se involucre en una actividad perjudicial en circunstancias específicas.
- Falta de garantías creíbles de que los productos sometidos a pruebas son idénticos a los componentes desplegados en plena operación. Al mismo tiempo, estos componentes pueden diferir de los entregados a todos los clientes, en particular, a los operadores de infraestructuras de información crítica.

La esencia de la advertencia de NUKIB y el mensaje central de las Propuestas de Praga finalmente se reflejaron en el "5G Security Toolbox" de la Unión Europea, lanzado en enero de 2020. Además de las medidas técnicas (TM), la Caja de Herramientas también incluyó un conjunto de medidas estratégicas (SM) y acciones de apoyo (SA)[16]. La Medida Estratégica 3 (SM03) formula la contribución de la República Checa a la seguridad 5G: **"Evaluar el perfil de riesgo de los proveedores y aplicar restricciones a los proveedores considerados de alto riesgo, incluyendo exclusiones necesarias para mitigar efectivamente los riesgos, para activos clave"**.

[15] Huawei Cyber Security Transparency Centre Opens in Brussels, https://www.huawei.com/en/news/2019/3/huawei-cyber-security-transparency-centre-brussels
[16] Cybersecurity of 5G networks EU Toolbox of risk mitigating measures, https://ccdcoe.org/uploads/2020/01/EU-200129-Cybersecurity-of-5G-networks-EU-Toolbox-of-risk-mitigating-measures.pdf

Conclusiones

La decisión sobre los proveedores de tecnología para las redes de telecomunicaciones 5G tendrá un impacto fundamental en los próximos años, especialmente a medida que el 5G alcance su máximo potencial para finales de esta década. Como tecnología, impulsará algunas de las funciones más críticas en cada país, como el transporte público autónomo o la próxima generación de procesos industriales. La elección de un proveedor confiable es de suma importancia. Las empresas chinas ofrecen soluciones tecnológicamente avanzadas y competitivas, pero el entorno político y legal en el que están obligadas y dispuestas a operar significa que no se puede confiar en ellas con nuestro futuro. Pasar por alto incluso los riesgos más básicos derivados de las relaciones de Huawei con el partido-Estado chino podría tener consecuencias graves para la seguridad nacional y la soberanía.