LITORALPRESS

Fecha: 27-02-2026
Medio: La Segunda
Supl. : La Segunda
Tipo: Noticia general
Título: Control estatal de las empresas de telecomunicaciones y espionaje, la pesadilla china de EE.UU.

Pág. : 2
Cm2: 675,2

Tiraje: 11.692
Lectoría: 33.709
Favorabilidad: No Definida

La lucha geopolítica entre Washington y Beijing

Control estatal de las empresas de telecomunicaciones y espionaje, la pesadilla china de EE.UU.

Servicios de inteligencia de varios países occidentales alertaron en 2025 que varias empresas chinas "ayudaron a Beijing" a perpetrar hackeos en 80 países.

Pablo Rodillo M.

La reacción de Estados Unidos al proyecto del cable chino que une a Valparaíso con Hong Kong era de esperar. China tiene una larga historia de espionaje en redes de telecomunicaciones y piratear teléfonos de funcionarios de alto rango de para obtener información sobre las operaciones estadounidenses.

En 2024 Washington acusó a China de apuntar a los teléfonos de varios políticos en una campaña de un grupo de hackers chinos llamada Salt Typhoon. El diario The New York Times informó que el actual presidente Donald Trump y el vicepresidente JD Vance estaban entre los objetivos de esta operación.

Y en agosto del año pasado, servicios de inteligencia de una docena de países, incluidos EE.UU., Francia, Alemania, Italia, Reino Unido y España aseguraron en un comunicado conjunto que un grupo hackers -incluidos los anteriores- respaldados por el gobierno chino estaban apuntando a infraestructura crítica y sistemas informáticos gubernamentales de otros países.

"Los datos robados a través de esta actividad con proveedores extranjeros de telecomunicaciones e Internet (ISP), así como las intrusiones en los sectores críticos, en última instancia, pueden proporcionar a los servicios de inteligencia chinos la capacidad de identificar y rastrear las comunicaciones y movimientos de sus objetivos en todo el mundo", aseguraron los servicios de inteligencia.

Una red vinculada a China que finalmente perpetró hackeos en organizaciones en más de 80 países, incluidos más de 200 objetivos en los Estados Unidos, como aseguró el FBI.

Y es que según este informe, "varias empresas chinas ayudaron a Beijing con sus ataques", pero nombró sólo a tres de ellas: Sichuan Juxinhe Network Technology Co., Beijing Huanyu Tianqiong Information Technology Co. y Sichuan Zhixin Ruijie Network Technology Co.

Estamos profundamente preocupados por el comportamiento irresponsable de las entidades comerciales nombradas con sede en China que ha permitido una campaña desenfrenada de actividades cibernéticas maliciosas a escala global", afirmó Richard Horne del Centro Nacional de Seguridad Cibernética de Reino Unido.

Así, "Beijing permitió a las empresas que trabajan para ella elegir objetivos a voluntad", aseguró Brett Leatherman, subdirector de la División Cibernética del FBI, a The Washington Post.

Además, por su parte, el Center for Strategic and International Studies (CSIS) y otros centros de análisis han advertido que una gran dependencia de cables submarinos gestionados por empresas chinas podría convertirse en un vector para espionaje o sabotaje en caso de conflicto.

Telecomunicaciones estatales

El año pasado, la Comisión Federal de Comunicaciones de Estados Unidos anunció un plan para endurecer su política sobre infraestructura digital estratégica: prohibir la conexión de cables submarinos que utilicen tecnología o componentes fabricados por empresas chinas. El trasfondo es que estos tendidos albergan actualmente más del 99?% del tráfico internacional de internet.

Hoy la industria de las telecomunicaciones en China está dominada por tres empresas estatales controladas por el Partido Comunista chino: China Telecom, China Unicom y China Mobile. Y las tres buscaron operar el cable que ha generado gran controversia en el país y de paso un impasse diplomático con Estados Unidos, siendo la última la que más ha avanzado en el polémico proyecto.

Por su parte, el discurso de las autoridades chinas para cualquier proyecto de este tipo suele presentarse en clave de beneficio económico inmediato. Inversiones, promesas de generación de empleo y la transferencia de tecnología. Pero al mismo tiempo, la falta de transparencia en su ejecución también es evidente.

Sin embargo y lo que preocupa a Estados Unidos y a otros países occidentales es que estas empresas estatales están obligadas por ley a entregar información al gobierno chino.

Como explicó una nota del portal argentino Infobae de septiembre del año pasado, siendo en esa oportunidad el primer medio que dio a conocer la noticia del cable chino a Chile, "la Ley de Ciberseguridad de China (CSL) obliga a los operadores de infraestructura crítica (que incluye a las empresas de telecomunicaciones) a almacenar localmente los datos y a cooperar con las autoridades chinas en caso de solicitudes de seguridad nacional. Esto incluye el derecho del Estado a realizar auditorías y requerir la entrega de información".

Mientras que -agrega Infobae- "la Ley de Inteligencia Nacional es una norma que complementa la CSL al exigir que cualquier organización o ciudadano apoye, asista y coopere con la labor de inteligencia del Estado. La ley no distingue entre actividades domésticas y en el extranjero, lo que amplía el alcance de la obligación".

A esto se suma, según el mismo portal trasandino, el Decimocuarto Plan Quinquenal de Informatización Nacional que establece de forma explícita que "China aspira a dominar las telecomunicaciones mundiales, no solo como proveedor de equipos, sino como operador de los canales de transmisión".

Así, mientras el "(cable) Humboldt (de Google) conecta Chile con Oceanía con socios identificados, el ChileChina Express aparece como proyecto en progreso con destino Hong Kong. La duplicidad de rutas hacia Asia, una con Estados Unidos y otra con China como actores principales, refleja la competencia geopolítica por controlar la infraestructura digital en la región", concluye Infobae.