LITORALPRESS

Fecha: 26-02-2026
Medio: La Segunda
Supl. : La Segunda
Tipo: Noticia general
Título: Cable con China: qué criterios deberán seguir los informes de seguridad que solicitó el Gobierno

Pág. : 7
Cm2: 671,7

Tiraje: 11.692
Lectoría: 33.709
Favorabilidad: No Definida

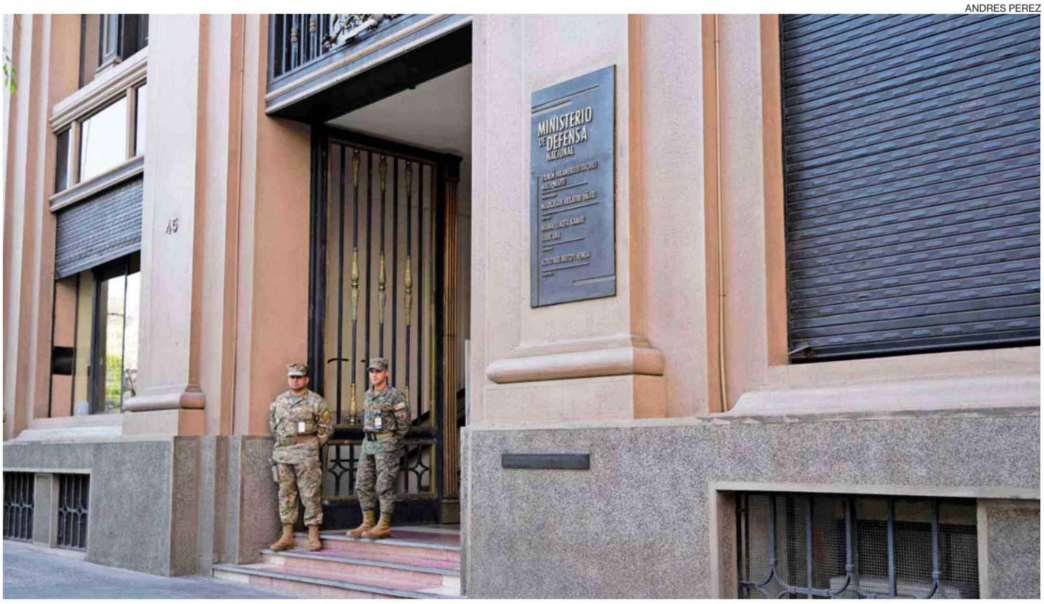
Ejecutivo los pidió a al menos tres instituciones

Cable con China: qué criterios deberán seguir los informes de seguridad que solicitó el Gobierno

La ANI, ANCI y el EMCO deberán determinar brechas de seguridad, defensa y soberanía en el proyecto de CMI, además de riesgos de hackeo.

Benjamín Celedón H.

ANDRES PEREZ



Luego de "anular" la aprobación del proyecto Chile-China Exprés a fines de enero, ante las advertencias de Estados Unidos por potenciales vulneraciones a la seguridad, el Gobierno pidió informes a, al menos, 3 instituciones: el Estado Mayor Conjunto de la Defensa (EMCO), la Agencia Nacional de Inteligencia (ANI) y la Agencia Nacional de Ciberseguridad (ANCI). Según el Ministerio de Transportes y Telecomunicaciones (MTT), estas medidas fueron "con el objetivo de incorporar al análisis la mayor cantidad de información posible y así tomar una decisión robusta y rigurosa", por lo que el contenido de dichos informes será lo que ayudará —en teoría— al próximo gobierno a determinar el destino del proyecto.

Específicamente, el embajador Brandon Judd detalló este lunes en un punto de prensa que habían advertido sobre "incursiones en los sistemas de telecomunicaciones chilenas por parte de de actores malignos extranjeros", lo que se suma a los antecedentes a recabar sobre defensa nacional, por el EMCO; y sobre inteligencia, por la ANI.

Riesgo de hackeo y soberanía

Hugo Galilea, director ejecutivo de la empresa de ciberseguridad Kepler, explica que "la ciberseguridad cubre tres puntos básicos: disponibilidad, integridad y confidencialidad. Son los tres puntos en los que debemos preocuparnos, sobre todo en infraestructura crítica, como es un cable transoceánico que nos conecta y por donde van a pasar los datos de todas las personas, las empresas y el Gobierno de Chile".

En esa línea, lo que debería analizar la ANCI para descartar vulneraciones es "que estos datos se manejen de forma confidencial, que nadie esté observando qué se está transmitiendo, que estén siempre disponibles y también la integridad de los datos, que significa que lo que se envía es lo mismo que la otra persona está recibiendo", dice Galilea.

Sobre el proyecto con China Mobile, el experto advierte que "estas son compañías privadas de China donde el gobierno chino tiene injerencia en que se le entregue cualquier información que ellos necesiten bajo requerimiento, y ahí es donde se está fallando en el tema de la confidencialidad".

Por otra parte, el Estado Mayor Conjunto (EMCO), organismo que asesora al Ministerio de Defensa y está conformado por miembros de todas las Fuerzas Armadas, deberá realizar un análisis más enfocado en la seguridad y defensa nacional.

"El informe del EMCO debiera contener aspectos relacionados con ciberseguridad, con la soberanía del fondo marino y la seguridad de las comunicaciones", explica un exalto funcionario de la institución, haciendo énfasis en los datos que se podrían obtener del fondo marino, que no solo contiene información privilegiada sobre riquezas minerales y pesqueras, sino también sobre infraestructura naval y submarina. "Eso para la seguridad es súper importante que no sea difundido", agrega un general del Ejército en retiro, experto en estos temas.

De hecho, en la misma línea, la Armada llevó a cabo ayer una fiscalización al buque científico chino Tan Suo Yi Hao, que llegó en enero a Valparaíso para liderar una investigación en conjunto con la U. de Concepción. La acción se realizó "bajo la normativa nacional e internacional vigente, verificando que sus actividades se desarrollen de acuerdo a las autorizaciones correspondientes", señaló el oficial a cargo de la fiscalización.

El informe de la ANI: "Mucho más político"

En contraste con los anteriores, de índole un poco más técnica, el informe restante es el de la Agencia Nacional de Inteligencia (ANI), que según otro exoficial ligado al mundo de la inteligencia, es una organización "mucho más política", lo que podría sugerir una inclinación proclive al clima político en que se evalúe el proyecto (en este caso, durante el próximo gobierno).

En esa línea, el documento no contemplaría solo elementos de defensa como el del EMCO, sino también consideraciones geopolíticas y hasta culturales en torno a la disputa de Estados Unidos con China. "Todo lo que son las decisiones militares son compromisos políticos. Lo técnico es una entrada más de lo político. No es solo lo técnico", agrega la misma fuente.

Defensa sufrió hackeos y filtraciones masivas de documentos en 2022 y 2023

En los últimos años, Chile no ha estado exento de vulneraciones a la seguridad, especialmente en el ámbito cibernético. La primera de ellas fue el 19 de septiembre de 2022, día de las glorias del Ejército, en que el grupo Guacamaya accedió a casi 400 mil documentos del EMCO. La acción gatilló la renuncia del jefe de la repartición y obligó a la entonces ministra Maya Fernández (Defensa), que al momento se encontraba en Estados Unidos de gira con el Presidente Boric, a retornar al país para encabezar un comité de crisis, además de iniciar una investigación sumaria en el EMCO y denuncias ante el Ministerio Público Militar y el Consejo de Defensa del Estado.

La segunda vulneración vino en mayo de 2023 —apenas 8 meses después— cuando el grupo hacker Rhysida ejecutó un ataque de ransomware (secuestro de datos que pide rescate para devolverlos) contra el Ejército. Según los atacantes, habrían vendido el 70% de los datos y dejado el resto (cerca de 360 mil documentos) para "consulta pública".