COLUMNA DE OPINIÓN

KENNETH PUGH,
senador de la República

La ciberdefensa activa

Este mes de mayo ha sido especialmente productivo en cuanto a actividades relacionadas con la ciberseguridad, tanto a nivel nacional como internacional. Se realizó en Santiago la primera versión de Cybertech South America, organizada por "El Mercurio"; luego las V Jornadas & Congreso RootedCON Capítulo Panamá, del Centro Criptológico Nacional de España (CCN-CERT), y esta semana se desarrolló la primera versión de Patagonia Ciber, en Puerto Varas, organizada por la nueva Agencia Nacional de Ciberseguridad (ANCI) y Fundación País Digital.

Sin embargo, el hito más importante desde el punto de vista geopolítico ocurrió el viernes 16 de mayo, cuando la Cámara Alta de Japón, con amplia mayoría, aprobó la nueva Ley de Ciberdefensa Activa de dicho país, otorgándole al gobierno facultades para que tome medidas proactivas para prevenir ciberataques graves.

El texto que se tramita en la nueva ley señala que el gobierno podrá, en tiempos de paz, adquirir y analizar las comunicaciones digitales entre países extranjeros a través de Japón y entre este y otros países. Si hay indicios de un ciberataque, la policía y las fuerzas de autodefensa podrán tomar medidas para neutralizar dichas amenazas.

A diferencia de lo que ocurre en el mar, donde el Derecho Internacional Marítimo reconoce el "paso inocente" de naves por aguas territoriales y obliga a submarinos a navegar aflorados o a no despegar helicópteros de naves de combate, en el ciberespacio no existen reglas que asimilen el tránsito de datos por un país soberano, que tiene el derecho a ejercer su "soberanía digital" e incluso la "legítima ciberdefensa".

Sin lugar a dudas, este hecho será analizado en todos los foros especializados de relaciones internacionales, ciberdiplomacia, geopolítica, gobernanza de internet (IGF) y ciberseguridad.

En este tema, Chile no se ha quedado atrás y gracias a un acuerdo político por unanimidad, ambas cámaras aprobaron la Ley Marco de Ciberseguridad, que permitió que el 1 de enero de 2025 comenzara sus actividades la ANCI, la que a fines de este mes promulgará el listado de empresas consideradas Prestadores de Servicios Esenciales (PSE) y Operadores de Importancia Vital (OIV), obligando a quienes queden sujetos a esta ley a reportar los ciberataques con una primera alerta en un plazo no mayor a tres horas, con aporte de información relevante del tipo de ataque y atacante dentro de las 72 horas y un informe completo a los 15 días. Estos criterios derivan de la transposición que el Congreso Nacional hizo de la Directiva NIS2 europea, siendo Chile también un pionero, en atención a que, hasta el momento, solo 11 de los 27 países que componen la Unión Europea han cumplido con la fecha para tener incorporada esta directiva en sus legislaciones nacionales.

El ejemplo de Japón de tomar la iniciativa y señalar que si su infraestructura crítica es atacada por delincuentes, el Estado puede responder con toda su capacidad activa, podría cambiar la asimetría actual con respecto a las acciones, por ejemplo, de "secuestro digital" de instalaciones que prestan servicios esenciales para la población o son críticos, tal como lo ha definido Chile. Para lograr esto, el país asiático se ha propuesto contar con cibercapacidades activas y defensivas "equivalentes o mejores que la de los principales países occidentales".

La ciberseguridad en el nuevo mundo digital es una herramienta geopolítica.

> "En el ciberespacio no existen reglas que asimilen el tránsito de datos por un país soberano, que tiene el derecho a ejercer su 'soberanía digital' e incluso la 'legítima ciberdefensa'".