Carlos Fazio

La visita relámpago a México del primer ministro de Israel, Benjamín Netanyahu, el jueves pasado transcurrió en un marco de gran opacidad y parquedad informativas.

Entre las empresas israelíes que acompañaron a Benjamín Netanyahu en su gira por América hay dos que desde hace tiempo cumplen un rol importante en el espionaje en territorio mexicano. Detrás del lenguaje diplomático de los mandatarios israelí y mexicano podrían estar encubiertos posibles acuerdos de colaboración policial y militar, en particular de ciberdefensa.

La visita relámpago a México del primer ministro de Israel, Benjamín Netanyahu, el jueves pasado transcurrió en un marco de gran opacidad y parquedad informativas y de manifestaciones de condena hacia el régimen de Tel Aviv, por sus políticas sangrientas y de apartheid contra la nación palestina en los territorios árabes ocupados.

El primer ministro israelí no hizo mención alguna del muro que pretende construir Donald Trump en la frontera entre México y Estados Unidos, mientras que en enero pasado, se había pronunciado a favor de la medida en Twitter: “El presidente Trump tiene razón. Construí un muro en la frontera meridional de Israel (la que separa al país de Egipto). Detuvo toda la inmigración ilegal. Gran éxito. Gran idea”. La cancillería mexicana expresó entonces su “extrañeza, rechazo y decepción” por las palabras de Netanyahu y el presidente israelí, Reuven Rivlin, aseguró que había sido un “malentendido”.

Según fuentes oficiales, Netanyahu y el presidente mexicano, Enrique Peña Nieto, suscribieron tres acuerdos para el “fortalecimiento” de la relación bilateral: uno sobre servicios aéreos, otro sobre exploración y uso del espacio con fines pacíficos, y un memorándum de entendimiento sobre cooperación internacional en temas de agua, agricultura, emprendimiento e innovación. La agencia de noticias Reuters mencionó “otros acuerdos” sobre proyectos conjuntos en materia de seguridad para reforzar la frontera sur de México con Centroamérica, y para trabajar conjuntamente “en materia de ciberseguridad, a fin de combatir delitos electrónicos”. Bajo el uso de un vago lenguaje diplomático y técnico, quedaron encubiertos posibles acuerdos de colaboración policial y militar, y de transferencia de información estratégica y operativa, acuerdos que de tiempo atrás han signado las relaciones bilaterales.

En particular, en materia de ciberseguridad y ciberdefensa; intercambio de datos sobre circulación financiera y flujos de cuentas bancarias del crimen organizado; metadatos de redes informáticas y sociales; aparatos de escucha y seguimiento aplicados a la seguridad pública y el espionaje político; análisis criminal y forense; monitoreo satelital de aparatología militar y otros tales.

VERINT. Una de las 30 compañías israelíes que acompañaron al premier Netanyahu en su reciente gira por las Américas fue Verint Systems, especializada en espionaje electrónico, con presencia en México desde hace tiempo. Bajo su antigua denominación de Verint Technology Inc, la firma fue subcontratada en 2007 por el Departamento de Estado norteamericano para realizar tareas de espionaje en el territorio mexicano en el marco de la Iniciativa Mérida.

Verint, encargada de desarrollar un “sistema de intervención de comunicaciones” en México –cuya información sería “compartida” en tiempo real con el gobierno de Estados Unidos–, fue introducida al país a través de la empresa Sogams (Sistemas Gerenciales Administrativos S A de C V).

Se trató de un primer caso concreto de tercerización de la “guerra” a las drogas y el terrorismo en México, que se practica desde el gobierno de Felipe Calderón. Según denuncias recogidas entonces por este corresponsal, la empresa
–constituida, entre otros, por ex militares israelíes y del Pentágono y ex agentes del Fbi– instaló ese año un sofisticado equipo de espionaje en las oficinas de la Subprocuraduría de Investigación Especializada en Delincuencia Organizada (Siedo).

Su misión fue monitorear o “captar” todas las comunicaciones privadas (correos, chat y

mensajes electrónicos a través de redes como Facebook, Twitter y Skype, faxes, llamadas telefónicas) con el pretexto de combatir “el crimen organizado y el terrorismo”.

Según pudo confirmar Brecha en 2007 con fuentes diplomáticas acreditadas en México, la Verint se regía por los lineamientos impuestos desde la embajada de Estados Unidos en México, en el contexto de un proyecto del Buró Internacional de Narcóticos y Asuntos de Aplicación de la Ley del país vecino. En buen romance, la Procuraduría General de la República (Pgr) hace el trabajo diario y Estados Unidos se queda con la información producto del “espionaje de cuello blanco” que realizan sus “contratistas privados”.

SOGAMS. Por esa vía, el Pentágono y las agencias de inteligencia de Estados Unidos e Israel acentuaron la dependencia de México en un área sensible para la seguridad nacional. La puesta en práctica de la Iniciativa Mérida (véase Brecha, 5-IX-08), con el monitoreo del espacio aéreo mexicano y el control de las telecomunicaciones, incluidas labores de escucha telefónica y el adiestramiento *in situ* de policías y militares en materia de terrorismo, sumado al nuevo protagonismo de las fuerzas armadas locales en la vida nacional, fueron esenciales en la conformación del actual régimen de “seguridad democrática” que, al igual que el impuesto en Colombia por Álvaro Uribe, fue manufacturado por Washington con parte de tecnología israelí.

En abril de 2008, el Centro de Investigación y Seguridad Nacional (Cisen, el servicio de inteligencia de México) había reconocido haber firmado al menos 14 contratos con la empresa Sogams. Según reveló entonces el diario estadounidense Los Angeles Times, el sistema de espionaje de Verint contaba con 30 “estaciones de monitoreo”, una base de datos telefónicos con capacidad de albergar 8 millones de sesiones y grabar 60 conversaciones al mismo tiempo.

Entonces, según la revista Contralínea, buena parte de la información sobre los contratos entre Sogams y el Cisen fue clasificada como de “carácter reservado” hasta por 12 años.

Otros clientes de Verint Systems en México –a través de Sogams–, fueron la Policía Federal Preventiva; la Oficialía Mayor del gobierno de Querétaro; el Sistema de Administración Tributaria, y Pemex Exploración y Producción. Desde 2015 la Verint abrió una oficina en la capital del país, por considerar que México representa un mercado estratégico en términos de inversión.

NSO GROUP. La empresa experta en espionaje informático Nso Group también acompañó a Netanyahu en su gira. En junio de este año protagonizó un sonado escándalo en México, cuando se detectó que a través de su malware Pegasus, instalado mediante un link que el usuario activa en forma inadvertida, convierte los teléfonos inteligentes en ojos y oídos de quien quiere espiar a sus propietarios. Así es posible rastrear sus conversaciones, correos electrónicos, mensajes de texto, llamadas, calendario, las teclas que pulsa, los detalles bancarios que revisa y dónde se encuentra.

Se divulgó entonces que la Pgr, el Cisen y la Secretaría de la Defensa Nacional (Sedena) le pagaron unos 31 millones de dólares a la firma Proyectos y Diseños Vme, para actualizar Pegasus y escalar sus capacidades de espionaje. Documentos también comprueban que Diseños y Proyectos Vme es una intermediaria entre el gobierno mexicano y la israelí Nso Group Technologies.

El caso es importante porque por primera vez se pudo documentar que el Cisen y la Sedena compraron Pegasus para realizar espionaje informático infectando los teléfonos de periodistas, activistas anticorrupción y de organismos defensores del consumidor, defensores de derechos humanos y líderes de partidos políticos opositores entre 2014 y 2016, de acuerdo con la investigación científica realizada por el laboratorio Citizen Lab de la Universidad de Toronto, Canadá (véase “Los paranoicos tenían razón” Brecha, 23-VI-17).

El Cisen, que depende de la Secretaría de Gobernación (Segob, Interior), utilizó Pegasus para vigilar y “consultar” el contenido de 1.250 blancos o dispositivos móviles. Una carta enviada por la propia Segob a la empresa intermediaria revela que el Cisen ya contaba con anterioridad con el software malicioso y que el objetivo del nuevo contrato correspondía a la “actualización y mantenimiento” de la plataforma para poder operar, a partir de setiembre de 2016, con nuevos sistemas operativos. Una factura de la Secretaría de la Defensa Nacional cifró el costo de la actualización en 1.113.600 dólares.

La literatura de la empresa proveedora indica que su software sólo puede ser adquirido por estados con una gestión limpia en materia de derechos humanos, pero el 10 de julio de 2017 el diario The New York Times divulgó un informe de Citizen Lab, según el cual Pegasus fue usado contra el Grupo Interdisciplinario de Expertos Independientes (Giei). El caso del Giei es especialmente grave dado que fue el propio Estado mexicano quien solicitó su presencia en el país para brindar asistencia internacional en el caso de los 43 estudiantes desaparecidos de Ayotzinapa y les aseguró inmunidad diplomática, por tratarse de un grupo designado por la Comisión Interamericana de Derechos Humanos (Cidh).