Reporte *Indigenous Surveillance*, capítulo Chile

Hackeo, implantación de evidencia y monitoreo redes sociales y metadatos a comunidades mapuche

Autoría:	Este reporte fue hecho para el proyecto *Indigenous Surveillance* por la investigadora Paz Peña.
Fecha y lugar de última versión:	09 de agosto del 2019 / www.indigenoussurveillance.net
Versión:	1.0
Derecho de autor:	

El año clave para comprender el uso de acciones de hacking sobre las comunidades mapuche en el sur de Chile es el año 2017. Al menos eso sabemos hoy, de acuerdo con las fuentes que se han publicado luego de que, a comienzos del 2018, se destapara el escandaloso y vergonzante episodio de la implantación de chats falsos en celulares de comuneros mapuche para inculparlos de atentados incendiarios por parte de Carabineros de Chile. La caída de la llamada Operación Huracán.

Gracias a la conversación de WhatsApp del 15 de marzo del 2017 que sostuvieron el coronel Marcelo Teuber, jefe de la Unidad de Inteligencia Operativa Especializada (UIOE) de Carabineros de La Araucanía, y su segundo al mando, el mayor Patricio Marín Lazo, se da luz a lo que tramaba Carabineros en la zona. En palabras de CIPER:

> "Introducir métodos hacker para penetrar las comunicaciones internas de grupos mapuche. Para ello se contrataría a un "asesor informático" y se crearía una unidad "de análisis forense informático".

Pero la verdad es que este tipo de métodos ilegales y de nefastos resultados tanto para la inteligencia del Estado, pero, por sobre todo, para los derechos humanos de los falsamente acusados, no solo fueron utilizados en la Operación Huracán. Todas estas acciones hacen pensar no solamente en las características de ensañamiento sobre un tipo de etnia, sino también sobre la necesidad urgente de reformar -en el marco de derechos humanos- la regulación de las actividades de inteligencia de nuestras policías.

Phishing en la Operación Huracán

A principios de marzo del 2017 fue creada, por el entonces general de Carabineros, Gustavo Villalobos, la UIOE de La Araucanía. No pasaría mucho tiempo para que se desentrañarse la intención de esta unidad de introducir "métodos hacker" para penetrar la comunicación de grupos mapuche.

Pero ¿cuáles eran esos "métodos hacker"? La verdad es que, revisando los antecedentes que hoy se disponen, el abanico es amplio y muy lejano a la más alta complejidad técnica que en un principio se hizo creer a la opinión pública. Una de las técnicas que más usó el UIOE fue el phishing que, para muchos especialistas, podría considerarse el método más común de engaño para apoderarse de antecedentes privados.

Los ataques de phishing son una forma de suplantación de identidad. Los ataques tradicionales intentan engañar a los objetivos para que proporcionen sus contraseñas creando un clon falso de, por ejemplo, la página de inicio de sesión de Google o Facebook. Si el objetivo es engañado para que ingrese su contraseña, el atacante "roba" sus credenciales y puede reutilizarlos para acceder a su cuenta de correo electrónico.

Esta técnica fue la que puso en práctica la UIOE a pocos días de su creación formal. El 27 de marzo 2017, se publicó la página de Facebook falsa "Lautaro Caupolicán" para hacer phishing a blancos mapuche y obtener así contraseñas de sus cuentas. Básicamente, el engaño consistía en enviar un correo electrónico disfrazado de una información de interés, que exige ingresar usuario y contraseña de redes sociales, y así apropiarse de esos antecedentes privados. Así se hizo el 22 de marzo de 2017 con la cuenta de la hermana de Jorge Huenchullán (dirigente de la comunidad de Temucuicui Autónoma) y uno de los acusados por la entonces Operación Huracán.

Pero quizás la operación más sistematizada de phishing en contra de las comunidades mapuche es el inexistente software "Antorcha", supuestamente creado por el asesor informático de la UIOE, Alex Smith, quien aseguraba que lo había desarrollado un para interceptar chats, incluso cifrados, sin tener acceso físico a los teléfonos.

De hecho, el 20 de septiembre del 2017, Gonzalo Blu, general de Carabineros y cabeza de la UIOE, entregó a la fiscalía el "Informe 130", que contenía el resultado de diligencias a cargo de esa unidad y donde se reproducen supuestas conversaciones entre algunos de esos dirigentes mapuche, sostenidas a través de distintos sistemas de mensajería instantánea, y que habrían sido interceptados por "Antorcha" entre el 1 y el 8 de agosto de 2017.

Aquello significó que el 23 de ese mes, en un operativo conjunto entre Carabineros y la Fiscalía de La Araucanía, se detuvieran ocho imputados (los hermanos Rodrigo y Jaime Huenchullan Cayul, Héctor Llaitul, Ernesto Llaitul, David Cid, Claudio Leiva, Martín Curiche y Fidel Tranamil) por su supuesta coordinación en ataques incendiarios en la zona sur (incluido los incendios de camiones de San José de la Mariquina donde, ya veremos, Alex Smith estaba implicado en la investigación). Se trataba de la denominada Operación Huracán, resultado de casi seis meses de investigación de Carabineros bajo la Ley de Inteligencia.

Hoy sabemos que el mismo día y hora en que personal de inteligencia de Carabineros periciaba los celulares de los dirigentes mapuche detenidos el 23 de septiembre, el capitán Leonardo Osses envió por correo electrónico a Álex Smith un archivo de texto con supuestas conversaciones entre Héctor Llaitul y otros implicados en la causa. Son los mismos diálogos que luego aparecieron en archivos .txt en los celulares de Llaitul. Tres peritajes posteriores al escándalo de la fallida Operación Huracán, indican que los archivos no son de mensajería instantánea y que habrían sido puestos en los teléfonos tras la incautación de la policía a través del software Oxygen Forensic (del que hablaremos más adelante en este mismo informe).

Pero Carabineros ya tenía antecedentes en noviembre de que los resultados de "Antorcha" eran sospechosos. Entre el 20 y el 25 de octubre de 2017, se sostuvo una reunión en las oficinas del mayor Patricio Marín Lazo en la UIOE con todos los peritos. Uno de ellos, Manuel Cavieres González, declaró a propósito de esta reunión:

> "Durante la reunión informé personalmente todo lo que habíamos realizado, y le comenté, a partir de lo hablado con Vásquez y los demás peritos, lo anormal que era haber encontrado archivos txt sin formato en algunos teléfonos. Sin embargo, el mayor Marín afirmó lo siguiente: 'pero estaba en el teléfono'. Yo me limité a contestar que sí, y no había más margen para analizar el asunto con él".

El engaño no solo quedaría en Chile. El 26 de septiembre de 2017, la policía filtró a El Mercurio diálogos falsos entre comuneros mapuche que apuntaban a que recibirían armamento desde Argentina en lo que se conocería como Operación Andes, la segunda parte de Huracán, que buscaba inculpar a comuneros por tráfico de armas. Las interceptaciones de esta operación eran a través del tristemente famoso software "Antorcha" y, gracias al especial ahínco del entonces general de Carabineros, Bruno Villalobos, llegaron al fiscal Sergio Moya que toma la causa.

Tres días después de esas filtraciones, el entonces subsecretario de Interior, Mahmud Aleuy, viajaba a Buenos Aires para reunirse con la ministra de Seguridad de ese país,

Patricia Bullrich, en los que se habló del supuesto tráfico de armas a los mapuche. Es más, el 12 de noviembre de ese año, un reportaje de Informe Especial (de la televisión nacional chilena) sobre la relación de organizaciones mapuche de Chile y Argentina incluyó una entrevista al fiscal argentino José Ignacio Jerez (el mismo que se coordina con el fiscal chileno Sergio Moya por Operación Andes), en la que este mantiene la tesis del tráfico de armas a comunidades mapuche: "Puede ser traspaso de armas o drogas. Son grupos que se financian a través del narcotráfico también".

Es más, meses después, el medio CIPER constató que la inteligencia argentina con Carabineros se compartían informes que, según ellos, explicarían la relación existente entre la RAM trasandina (Resistencia Ancestral Mapuche) y la CAM chilena, al igual que los informes de análisis de las redes sociales de las familias de Santiago Maldonado y de Facundo Jonas Huala realizado por la empresa argentina Voyager Labs.

Así, llegó el 2 de diciembre del 2017, y en el sector La Cascada del Parque Nacional Vicente Pérez Rosales, en la Región de Los Lagos, policías, fiscalía y tribunales no logran encontrar ningún indicio de tráfico de armas. Todo, hoy sabemos, era falso.

Sin embargo, el comienzo del fin del engaño en la Operación Huracán se remonta poco después de las detenciones producidas en septiembre del 2017. A inicios de octubre de ese año, Patricio Marín de la UIOE había informado a la Fiscalía Nacional una presunta filtración desde la oficina del Fiscal que llevaba la investigación post Operación Huracán, Luis Arroyo, a través de la abogada Mónica Palma, a los implicados en los atentados. Según La Tercera, durante ese mes, hasta inicios de noviembre, Inteligencia interceptó el teléfono de Palma y supuestamente encontró mensajes que comprometían a Arroyo (lo que después se comprobó que era otra mentira de la UIOE). Así, el 11 de diciembre, la Dirección Nacional de Inteligencia, Drogas e Investigación Criminal de Carabineros, remitió al fiscal nacional, Jorge Abbott, el "Oficio N°202", informándole de supuestas filtraciones desde la fiscalía y la Agencia Nacional de Inteligencia (ANI) a un tercero conectado con la Coordinadora Arauco Malleco. Por esta razón, la Fiscalía Nacional debió periciar nuevamente los teléfonos de los comuneros y, casi por casualidad, descubrir que las conversaciones que motivaron su detención habían sido implantadas por la UIOE.

Toda la maquinaria de inteligencia de Carabineros para perjudicar a los comuneros mapuche terminó en enero de 2018, cuando el Ministerio Público finalmente informó a la opinión pública que había descubierto la manipulación de las pruebas que incriminaban a los detenidos y anunció el cierre de la Operación Huracán sin acusados.

Ya en plena investigación judicial, el 6 de mayo de ese año, la PDI entregó su informe final sobre las irregularidades presentes en la Operación Huracán, determinando que "Antorcha" nunca existió. Poco después, cuando ya había poco que desmentir, Alex Smith admitió que el software "Antorcha" no era real. En una entrevista con La Tercera, dijo que en su labor intentaba hackear a blancos mediante una mezcla artesanal y poco efectiva de aplicaciones y que "ese nombre de Antorcha se puso en diciembre, antes no tenía nombre. Lo que hacía lo llamábamos hacer un Lautaro". ¿Qué hacía, entonces, "Antorcha"? "Mandar un phishing con keylogger. A veces no teníamos correo y se conseguían ellos los datos de los blancos con Banco Estado". Luego, se extiende sobre qué era "Antorcha":

> "Este era un procedimiento de phishing, malware y keylogger. No era un software como el que usa la PDI (Policía de Investigaciones). Mezclamos aplicaciones y después se le puso

> Antorcha. Recién la estábamos validando en diciembre. La verdad es que no se podía basar ningún caso en Antorcha, pero servía para hacer algo de inteligencia".

Los keyloggers son un spyware malicioso que se usa para capturar información confidencial, como contraseñas, a través del registro de cada tecla que se pulsa en un dispositivo, como un computador. Smith, en esa misma entrevista, dice algo clave sobre sus tareas en la UIOE:

> "Nació la necesidad de intervenir redes sociales. Lo más fácil para mí era el phishing. Comenté que se podía hacer y pregunté si era legal, me dijeron que por una ley, la de inteligencia, sí. Como era legal, empezamos a enviar phishing a distintos blancos. Se enviaba a un correo con una imagen que definía el capitán Osses, que conocía los blancos y sus gustos, buscaba una imagen que a esa persona le pudiera llamar la atención. Se hacía harta contrainteligencia también. Caía con suerte el 30% y entrabamos al correo y Facebook. Después piden whatsapp, y ahí usamos keylogger, también tuvimos una efectividad baja. Lo que quedaba registrado era lo que el blanco escribía. Después enviábamos un malware, que tenía un niño de España. Nunca desencriptamos Whatsapp, lo que hacía el malware era, a veces, reenviar lo que se conversaba".

A propósito de Smith, hoy sabemos que ya en enero de 2017, dos funcionarios de la Dipolcar hicieron un documento donde advertían las deficiencias informáticas de Álex Smith Leay. El informe, no obstante, y por circunstancias aún no aclaradas, estuvo perdido por 20 meses.

Implantación de evidencia en celulares

Como se indica en la sección anterior de este reporte, tres peritajes hechos luego de que se destapara el escándalo de la Operación Huracán indican que los mensajes incriminatorios a los comuneros mapuches habrían sido puestos en sus celulares después de la incautación que hizo de los aparatos la policía, a través de un software llamado Oxygen Forensic. Vale la pena concentrarse en este aspecto porque muestra evidencias de cómo Carabineros orquestó el engaño.

El 29 de agosto del 2017, uno de los dueños de la empresa intermediaria XMart Lab -Gonzalo Paredes Quezada- fue contactado directamente por el mayor Patricio Marín de la UIOE, quien le pidió cotizar el software Oxygen Forensics Rugged Kit, que incluía una tablet forense cargada con el software Oxygen Forensic Extractor y una licencia adicional Oxygen Forensic Detective, además de una capacitación para tres usuarios en la que aprenderían a usar la herramienta, hacer gestión de la evidencia y presentarla en tribunales.

Oxygen Forensic es un programa destinado a "recupera todos los datos de las aplicaciones vitales del dispositivo móvil con iOS, el sistema Android, BlackBerry 10, Windows Phone 8". Como indica La Tercera, en su última versión el software "agregó la capacidad de extraer datos adicionales de WhatsApp Cloud. Ahora los expertos forenses pueden adquirir información sobre mensajes eliminados de chats privados y grupales, imágenes de perfil y mensajes de estado del propietario y contactos de la cuenta, mensajes originales incrustados en la respuesta, mensajes de difusión, etc.", funciones que, según el mismo medio de prensa, son similares a las que realizaba "Antorcha" según Alex Smith.

Oxygen Forensics es la empresa que desarrolla este tipo de tecnologías y está basada en Virgina, Estados Unidos. De acuerdo con Privacy International, compañías como "Cellebrite, MSAB y Oxygen Forensics venden software y hardware para hacer cumplir la

ley. Una vez que su teléfono está conectado a una de estas herramientas de extracción de teléfonos móviles, el dispositivo extrae, analiza y presenta los datos contenidos en el teléfono. Los datos que pueden extraer estas herramientas y el método utilizado dependerán del sistema operativo, las características de seguridad y el modelo de teléfono".

La compra de un software de estas características podría ser considerada natural, de acuerdo con las labores de inteligencia de un organismo como Carabineros. No obstante, el método de la compra parece al menos sospechoso. Y es que el 1 de septiembre del 2017, el mayor Marín llegó a la empresa intermediaria, XMart Lab, y de acuerdo con Paredes Quezada:

> "[...] con el dinero en efectivo equivalente al monto cotizado, con el objeto de adquirir el producto seleccionado. Recuerdo que al momento de pagar el producto el mayor Marín extrajo desde una maleta un sobre plástico sellado con el nombre del 'Banco Central', que contenía billetes con una nominación de $20.000. Al abrirlo se contabilizó la suma de $20.000.000. Luego, extrajo un fardo de billetes de $10.000 (diez mil pesos) y pagó la diferencia".

Ese mismo día se emitió la factura electrónica N° 13 de la empresa Xmartlab Limitada a Carabineros de Chile. Paredes Quezada asegura que le comentó a Patricio Marín que no era habitual que un cliente pagara en efectivo, "a lo que él respondió que su lugar de trabajo era una unidad de Inteligencia y que el procedimiento debía efectuarse de esa forma".

Asimismo, como afirma el medio Interferencia, los fondos para la compra del software fueron aprobadas personalmente por el general de Carabineros en este entonces, Gustavo Villalobos, y que salieron de la partida de gastos reservados que manejan los General Directores. Además, el medio afirmó que XmartLab es una empresa que no figuraba en este entonces en el listado de Chile Proveedores. Más aún, el general Villalobos ocultó deliberadamente esa información a la Contraloría General de la República, "probablemente, en un intento por no dejar rastros de esas operaciones de inteligencia que desembocaron en la Operación Huracán".

Monitoreo de actividades en Internet

El monitoreo de actividades en Internet tiene múltiples formas cuando se trata del espionaje a comuneros mapuche, aún más allá del phishing que, como se ha explicado en este reporte, se ha utilizado en diferentes plataformas. Lo que es aún más grave, muchos de estos monitoreos ocurrieron hacia medios de comunicación y periodistas mapuche por parte de la UIOE, con métodos que hoy están en entredicho.

De acuerdo con la investigación de CIPER, por ejemplo, se registra que en junio del 2017, la UIOE hizo un rastreo de Mapuexpress.org, uno de los medios mapuche más reconocidos. El 13 de junio de ese año, Álex Smith envió al correo del capitán Leonardo Osses "un somero análisis" del sitio web, como lo califica CIPER, además de las cuentas de Facebook y Twitter del medio y un punteo de los dirigentes mapuche que eran usuarios de Mapuexpress.org, incluyendo el nombre de Patricio Melillanca como responsable del hosting del sitio. Además, en su informe, Smith "también afirmó haber identificado el lugar desde donde se emitirían sus mensajes de Twitter: en la precordillera de Las Condes, en medio de un bosque".

De acuerdo con el mismo reportaje de CIPER, otro comunicador mapuche que estaba en la mira de la UIOE era Richard Curinao, editor responsable del portal Werken.cl, el que se

define como "medio de comunicación informativo del pueblo Mapuche". Por un lado, el 19 de abril de 2017 el capitán Leonardo Osses recibió un correo electrónico de Álex Smith con un link de werken.cl, donde se informaba de un listado de 37 presos políticos mapuche, una dirección de Gmail, su usuario y su contraseña. Según CIPER, estos datos fueron obtenidos por Smith con xploitz.net, un "sitio web utilizado por escolares para hackear cuentas de redes sociales".

Por otro lado, en los reportes de las interceptaciones supuestamente capturadas por el que hoy sabemos falso software "Antorcha", aparecen chats de Curinao para coordinar agitaciones durante la visita del Papa Francisco a Temuco en enero del 2018, los que el mismo Curinao desmiente. En el 2010, Richard Curinao ya había sido allanado por la PDI, lo que organizaciones acusaron como un atentado a la libertad de expresión.

En declaraciones a la radio Juan Gómez Millas, Curinao dijo que, al enterarse de este informe de CIPER, se sintió vulnerado y que su sospecha era que los policías realmente buscan las fuentes de su trabajo periodístico. Finalmente, el 16 de marzo del 2018, el editor del sitio Werken.cl presentó una querella -que fue declarada admisible por el Juzgado- pues acusa haber sido víctima de revisión ilegal de su correo electrónico y celular.

Pero el monitoreo de las actividades en Internet por parte de la UIOE también llega a los comuneros mapuche. Por ejemplo, hoy sabemos que Camilo Catrillanca (asesinado el 14 de noviembre del 2018 por la intervención de agentes del GOPE que eran parte del famoso Comando Jungla) estaba en la mira de la UIOE pues esta unidad, ya a mediados del 2017, le había dedicado un informe de seguimiento de redes sociales. CIPER afirma que:

> "En el informe "secreto" revisado por CIPER no hay ni un solo hecho que vincule a Camilo Catrillanca con delitos comunes y tampoco con actos terroristas. Lo que lo puso en el radar de la policía fue el destacado rol que Catrillanca ejercía y, desde hacía años, en su comunidad, en la defensa de su identidad cultural [...] El único dato que aparece en ese informe de Inteligencia que vincule a Camilo Catrillanca con algún ilícito, es ser amigo en redes sociales de Fabián Llanca. La información que la UIOE entrega sobre Llanca era que lideraba una *"organización criminal"* a la que se "*asociaba*" al "*robo de vehículos, tráfico de drogas, desórdenes, porte de armas y munición, atentados incendiarios de camiones, casas y galpones; y al homicidio frustrado a carabineros de servicio"*.

Asimismo, hay informes que prueban que agentes encubiertos de Carabineros se han infiltrado en las comunidades mapuche gracias al uso de redes sociales. La Operación Tarzán, del año 2013 y en la que estaba implicado Leonardo Osses que hoy conocemos por la UIOE, tenía -en palabras de CIPER- los siguientes objetivos:

> "A través de las redes sociales de internet tomar contacto con comuneros pertenecientes a comunidades radicales (...) además de colaboradores y simpatizantes de la causa mapuche, en especial del sexo femenino, con el fin de concretar lazos afectivos". Luego de creados esos lazos el agente debía lograr "lazos de confianza" con los comuneros, "efectuando visitas a las comunidades, participación en marchas afines a la causa, ceremonias religiosas de la etnia, visitas a los denominados presos políticos mapuche", y cualquier otra acción que no pusiera en riesgo su vida ni transgrediera "la normativa vigente".

El caso recuerda a los agentes encubiertos que en Brasil usaron redes sociales -incluido plataformas de citas- para infiltrar protestas en contra de Michel Temer. Son escalofriantes, además, el tipo de conclusiones que, en el caso de Operación Tarzán, el

agente encubierto hace. Por ejemplo, reportó sobre un niño de 13 años: "Será un futuro "Machi" y subversivo de la familia **** ****, ya que mantiene bien arraigado sus principios con la causa mapuche".

Por su parte, el 7 de agosto del 2018, la ONG Defensoría Popular denunció que uno de sus integrantes, el abogado Lorenzo Morales Cortés, sufrió una masiva intervención cibernética de sus comunicaciones y redes sociales, lo que fue puesto en conocimiento de la Policía de Investigaciones. Además, precisaron que este ataque "se suma a otras interceptaciones de comunicaciones de integrantes de la organización en los últimos meses, incluyendo situaciones sutiles que, sin explicación aparente, han sufrido de parte de desconocidos". Lo que hace todo más preocupante no es solo que esta denuncia ocurre con la UIOE ya desmantelada, sino además que Lorenzo Morales es parte de la defensa de integrantes de la CAM.

Acceso ilegal de metadatos de las comunicaciones

En el marco del escándalo público luego de saberse el montaje detrás de la Operación Huracán, el medio de prensa CIPER descubrió el funcionamiento de la casa Hochstetter, donde operó, de forma secreta desde 2016 y hasta febrero del 2018, el centro de escuchas telefónicas de la UIOE de Carabineros. Además de éstas, Carabineros también tenía acceso a la información que entrega el software VIGIA, que es utilizado por las compañías telefónicas en Chile para guardar por un año la metadata de las comunicaciones, tal como hoy les obliga la ley vigente (artículo 222 del Código Procesal Penal).

¿Por qué los metadatos son de interés investigativo si no es la comunicación misma? Edward Snowden, que denunció la vigilancia masiva de Estados Unidos a través del uso de metadatos, recomienda que cada vez que veamos la palabra "metadatos" o "datos sobre las comunicaciones", la reemplacemos por un "registro de actividad". Efectivamente, como dicen en Privacy International, los metadatos revelan aún más de nosotros que lo que jamás podrán hacer los contenidos mismos de nuestras comunicaciones:

> "Tomados por separado, los pedazos de metadata parecer no tener muchas consecuencias. Sin embargo, los avances tecnológicos implican que los metadatos pueden ser analizados, extraídos y combinados de manera que sean increíblemente reveladores. Cuando se tiene acceso a ellos y se analizan, los metadatos pueden crear un perfil completo de la vida de una persona: dónde está en todo momento, con quién habla y por cuánto tiempo, sus intereses, condiciones médicas, puntos de vista políticos y religiosos y hábitos de compra".

En este contexto, hace años existe interés por parte de las policías y de los gobiernos por modificar el decreto 142 sobre metadatos y aumentar el plazo de retención, sobre todo en el marco de las investigaciones en La Araucanía. Así se constataba, por ejemplo, en las críticas de la normativa que llevaron a que el 25 de agosto del 2017, el gobierno de Bachelet, encabezado por su subsecretario del Interior, Mahmud Aleuy, firmara un decreto para que los metadatos en Chile fueran ahora guardados por las telecos por dos años (el que terminó bautizándose como "Decreto espía" y fue finalmente frenado por la Contraloría).

> "[...] había causas, como, por ejemplo, de La Araucanía, en las que transcurrido más de un año aparecían datos de teléfonos o blancos que era necesario indagar y se pedían los datos comunicacionales a las compañías y estas se escudaban en el 222 del Código Procesal Penal, porque lo interpretaban como máximo un año y la norma es interpretable, pues dice a lo menos un año".

La retención de metadatos en Chile funciona con la cooperación de las empresas de telefonía. El software VIGIA permite a las empresas cumplir la ley y guardar metadatos como el tráfico de llamadas del número, tráfico de mensajería de texto (SMS) y de imagen (MMS), su ubicación georeferencial, entre otros. De acuerdo con información del 2016 de la Fiscalía nacional, VIGIA es usado en el país por las empresas Movistar, Entel, Wom y Claro.

Es importante constatar que la empresa que desarrolla este software, Suntech, es de origen brasileño y también tiene presencia en otros países ofreciendo los mismos productos y servicios a empresas de telecomunicaciones. Suntech, además, aparece en el banco de datos de empresas que facilitan la vigilancia masiva, que publicó Wikileaks en el 2011.

Según explicó públicamente el director de la Unidad Especializada en Tráfico Ilícito de Estupefacientes y Sustancias Sicotrópicas de la Fiscalía Nacional, Luis Toledo, esta herramienta permite gestionar de manera inteligente toda la información que deriva de una interceptación telefónica, autorizada judicialmente:

> "A través de la plataforma Vigía existen una serie de datos que se administran, como el día, la hora, la geolocalización y además cada una de las personas y las direcciones web que se encuentra comunicando instantáneamente entre ellas. Esta herramienta permite gestionar de manera inteligente todos estos datos con el objetivo de mejorar la investigación criminal".

Debido a que estamos hablando de una intrusión a la privacidad de las personas, en Chile se requiere que un juez autorice previamente el acceso de la policía a los metadatos de las comunicaciones retenidas por las empresas de telecomunicaciones. No obstante, y de acuerdo con medio CIPER, distintas personas que han integrado o integran equipos de inteligencia, testifican que existe una vía paralela -y fuera de la ley- para obtener la metadata de las comunicaciones:

> "Como en casi todas las compañías telefónicas los encargados de la seguridad y de dar acceso a las interceptaciones son oficiales de Carabineros en retiro, se posibilitan los tratos privados entre efectivos de inteligencia y ejecutivos de las compañías telefónicas para acceder a información absolutamente privada de ciudadanos sin autorización".

La polémica sobre el uso de las comunicaciones por parte de la UIOE no termina ahí. En la denominada operación Huracán 2 hay antecedentes alarmantes. Esta operación comenzó el 28 de agosto del 2017, cuando ocurrió una quema de 29 camiones de la empresa Sotraser en San José de La Mariquina. Para esa investigación, el asesor de la UIOE, Alex Smith, desarrolló la aplicación "Tubicacion.cl" (la que, por lo demás, también está en entredicho debido a una diferencia de fechas entre el atentado y su registro en NIC Chile). Smith declaró:

> "Lo que me pedían era desarrollar una herramienta que permitiera determinar cuántos teléfonos habían en un determinado lugar y dónde se encontraban estos. El objetivo del software era forense, iba a ser administrado por el Labocar, para ese efecto se compró el hosting y el nick "tubicación".

Con esta aplicación, se elaboró un informe de posicionamiento de celulares para la ubicación de uno de los imputados, el comunero Patricio Antiago. Pero los resultados de Tubicacion.cl eran falsos. La Fiscalía Regional de Los Ríos logró establecer que el comunero, casi a la misma hora del atentado incendiario, estaba siendo controlado por el

mismo personal de Carabineros que fiscalizaba el cumplimiento del arresto domiciliario total decretado en su contra por una causa de porte ilegal de municiones.

Pablo Arduain, el abogado defensor de Patricio Antiago, agrega que no es esa la única prueba que les hace sospechar que la Fiscalía tenía a su cliente en la mira, más allá de las responsabilidades reales:

> "En el Poder Judicial existe una solicitud de obtención de tráfico de llamadas, no de interceptación telefónica, en que se solicitaban copias de los tráficos de llamadas no del teléfono de don Patricio, porque él no ocupaba celular, sino que del número de su madre. [...] Estimamos que el blanco directo no era ella sino que era una manera de llegar a don Patricio".

Cuando el Estado chileno hackea

Cabe recordar que la Ley de Inteligencia regula el actuar de los organismos de inteligencia en el marco de una investigación que tenga por objeto el resguardo de la seguridad nacional y proteger al país de las amenazas del terrorismo, el crimen organizado y el narcotráfico. Los procedimientos especiales de obtención de información para los organismos de inteligencia están regulados por el artículo 23, que señala que la información a recabar debe resultar "estrictamente indispensable para el cumplimiento de los objetivos del Sistema y no pueda ser obtenida de fuentes abiertas", imponiendo un elevado estándar para la aplicación de tales procedimientos. Otro de los requisitos esenciales de la autorización judicial otorgada por un Ministro de Corte de Apelaciones competente, que dicha resolución debe incluir "especificación de los medios que se emplearán", además de la individualización de las personas a quienes se aplica la medida y las limitaciones temporales de su aplicación.

No obstante, como afirman una serie de organizaciones de la sociedad civil especializadas, la Operación Huracán lleva a concluir que los mecanismos contenidos en la Ley de Inteligencia "resultan insuficientes para cautelar que no se vulnere en su aplicación el respeto por la privacidad y la inviolabilidad de las comunicaciones de ciudadanos amparados por el principio de presunción de inocencia. La ley de inteligencia carece controles externos que permitan precaver los excesos de los organismos de inteligencia en su aplicación, y el poder judicial está fallando en aplicar un control sustantivo de las actividades de inteligencia al autorizarlas".

Por ejemplo, Smith afirmó que la UIOE de Carabineros le confirmó que los métodos detrás de "Antorcha" (phishing, malware y keylogger) eran legales. Aquello es altamente discutible según especialistas en la materia. Pablo Viollier, abogado de la ONG Derechos Digitales, en una intervención realizada en octubre del 2018 ante la "Comisión investigadora sobre actuación de organismos policiales, de persecución criminal y de inteligencia en Operación Huracán" de la Cámara de Diputados, fue claro:

> "En el caso particular de Operación Huracán, la prueba supuestamente obtenida tampoco cumple con el estándar señalado en el artículo 24 de la Ley de Inteligencia. De acuerdo a Carabineros, el supuesto malware instalado en los aparatos de los imputados fue introducido a través de una técnica denominada phishing, una forma fraudulenta de obtener información confidencial como nombres de usuario y contraseñas disfrazándose como una entidad confiable en una comunicación electrónica. Este uso del engaño fraudulento, propio de los delincuentes informáticos, con el fin de instalar un programa malicioso (malware) no se encuentra amparado ni en la Ley de Inteligencia ni en el Código Procesal Penal".

Esto demuestra que, a sabiendas de que el procedimiento era ilegal, el Estado de Chile, a través de Carabineros, realizó acciones de hackeo que, por lo demás, terminaron urdiendo un montaje contra conocidos dirigentes mapuche. Pero la responsabilidad del Estado en el uso de estos métodos de hackeo ilegal, lamentablemente, no queda ahí.

El 9 de agosto del 2017, el magistrado Aner Padilla de la Corte de Apelaciones concedió una "autorización retroactiva" a Carabineros para realizar las interceptaciones en la "Operación Huracán" bajo la Ley de Inteligencia. Según se lee en la carpeta, "incluso aquellas comunicaciones e informaciones relevantes a las que se tenga acceso o se puedan obtener, y que se hayan producido o generado con una antelación máxima de 30 días, contados desde esta fecha y hora". Fue esa figura de "autorización retroactiva" la que permitió que los diálogos supuestamente interceptados a comuneros mapuches entre el 1 y el 8 de agosto de 2017, fueran consideradas pruebas válidas ante la ley.

El problema es que la "autorización retroactiva" de interceptación de comunicaciones no existe en Chile. Como le dijo a La Segunda el ex subdirector de la Agencia Nacional de Inteligencia (ANI), Pedro Anguita, los jueces no pueden autorizar intervenciones ya practicadas por los organismos de inteligencia, pues el artículo 28 de la Ley 19.974 dispone que la resolución judicial que autoriza debe especificar los medios que se emplearán, individualizar personas a las que se les aplicará la medida y el plazo; exigencias que sólo pueden pedirse antes de la ejecución de las medidas intrusivas. Las "autorizaciones retroactivas", entonces, serían inconstitucionales e ilegales.

Eduardo Painevilo, representando en la comisión investigadora de la Cámara de Diputados (que sesionó el 22 de octubre del 2018) al abogado Sebastián Saavedra, defensor titular del machi Fidel Tranamil, dijo que es en agosto del 2017 donde "se marca un antes y un después" en las peticiones de interceptación de comunicaciones en el marco de la Operación Huracán:

> "… hacia atrás fueron los típicos "pinchazos", o sea, interceptaciones telefónicas; luego, desde agosto hacia adelante, las solicitudes de intervención incluyen la petición expresa de interceptar (mensajes de) WhatsApp, Telegram y aquellas redes sociales en las cuales se pueda tener comunicación. Eso se hace porque supuestamente en agosto ya existía la posibilidad de intervenir WhatsApp por parte de la unidad inteligencia, lo cual, en la nueva investigación, se ha comprobado que es totalmente falso".

En esa misma sesión, Viollier ahondó sobre la falta de un control estricto de los jueces ante los requerimientos de interceptación telefónica bajo la ley de inteligencia:

> "Lo que se ve de la resolución de la Corte de Apelaciones de Temuco -no se sabe si es algo que se replica en el resto de las jurisdicciones- es que la corte simplemente está haciendo, en un proceso que además es secreto, un análisis completamente formal. ¿Es usted una agencia de inteligencia? Sí. ¿Me está diciendo qué es lo que va a ser, en términos más o menos amplios? Sí. Entonces, vaya y hágalo. En consecuencia, no se está cumpliendo el principio de que exista un control respecto de las actividades que están realizando las agencias de inteligencia".

Pero las irregularidades de la actuación del Estado chileno siguen. Por ejemplo, en un correo electrónico que fue obtenido de forma anónima por el fiscal Arias, el fiscal Sergio Moya envió un email al correo personal del Mayor (r) de Carabineros Patricio Marín con fecha 13 de diciembre del 2017, dando instrucciones sobre las indagatorias en la causa de la

Operación Huracán y donde, como se ve en el texto, estaba al tanto de la implantación de pruebas:

> "Quién lo firme seguramente declarará en las investigaciones. Lo más probable es que lo pericien, por lo que hay que sugerir que se pericien por Labocar para no revelar la técnica investigativa, pues si se revisan por PDI se entregará a Cibercrimen, los que informarán que no es posible pichar WhatsApp, y así se termina la investigación".

Asimismo, a este correo se suman una serie de mensajes vía WhatsApp que darían cuenta de la estrecha colaboración entre los fiscales Marín, Moya y otros funcionarios de Carabineros.

Vigilancia racista

El panorama se pone aún más desalentador, cuando sabemos que a una Ley de Inteligencia que muestra deficiencias, hay capacidades de espionaje electrónico mucho más sofisticado por parte de las policías. Y es que de casualidad, y gracias a una filtración internacional, desde el 2015 sabemos que la PDI adquirió un software de espionaje electrónico por más de US$ 2,8 millones a la empresa Hacking Team (que vendió su sistema Galileo pero que en Chile el fue rebautizado como Phantom). De acuerdo con su comunicado de prensa:

> "Fue adquirida en el marco de un proyecto de modernización del área tecnológica de la PDI, cuyo objetivo era incrementar sus capacidades operativas en la investigación de crimen organizado, terrorismo internacional y narcotráfico a gran escala, considerando que cada día la delincuencia organizada es más sofisticada y cuenta con importantes soportes logísticos y económicos".

La evidencia sistemática acá expuesta deja al Estado chileno muy cerca de prácticas de vigilancia ilegal de estados como el de Egipto que, bajo el gobierno de Abdel Fatah al Sisi, lanzó una ola de ciberataques basados en phishing a personas defensoras de derechos humanos, ONGs y periodistas; o a México, que con el gobierno de Enrique Peña Nieto, se gastó al menos 80 millones de dólares para vigilar las comunicaciones electrónicas de, de nuevo, personas defensoras de derechos humanos, ONGs y periodistas. La diferencia, no menor, es que las prácticas ilegales sistemáticas en Chile han sido contra personas y defensores de una etnia en particular: la mapuche.

****