Herramientas de Vigilancia Digital Identificadas en Centroamérica

FUNDACIÓN Acceso

Con el apoyo de

Hivos people unlimited

Digital Defenders Partnership

Fundación Acceso, 2020
Autor: Rafael Bonifaz,
Revisión: Larraitz Lexartza y Tanya Lockwood.
Con la colaboración de Rodrigo Baires.

Disclaimer

Este artículo hace referencia a algunas herramientas tecnológicas, disponibles para los gobiernos, que podrían ser empleadas con fines de vigilancia. Sin embargo, el hecho que estén disponibles no implica necesariamente que se estén empleando con dicho fin. El objetivo de este artículo es dar a conocer la existencia de dichas herramientas para educar a la ciudadanía, y para que se pueda abrir un debate sobre la pertinencia de su uso y los riesgos que implicaría su abuso.

Es importante notar que las herramientas presentadas en este artículo no son todas las existentes, son solamente auquellas de las que se tiene conocimiento de su existencia por fuentes públicas.

Toda la información disponible en este artículo ha sido utilizada como bibliografía en base a fuentes de acceso público.

Agradecimiento

Agradecemos a Hivos y DDP su apoyo para la realización de esta investigación.

Introducción

Internet permite acceder a cantidades ilimitadas de conocimiento, y comunicarse de forma barata y rápida a nivel mundial. Sin embargo, también permite una vigilancia direccionada o global a gran escala. La Internet no fue diseñada teniendo en cuenta la privacidad y seguridad de las comunicaciones. Cuándo se visita un sitio web, se envía un mensaje de texto o correo electrónico, se interactúa en redes sociales, se sube un video u otro tipo de actividades en línea los datos privados de las personas pueden ser fácilmente monitoreados, interceptados, recolectados, almacenados y accedidos por diversos actores.

Más aún, cada vez que se utiliza Internet, se deja información personal voluntariamente, por ejemplo, en las publicaciones de redes sociales. También se hace de manera involuntaria, a través de los metadatos que se registran con la actividad de quiénes usan Internet. Por ejemplo, quién se comunica con quién, las páginas web visitadas o la ubicación, entre otros patrones de comportamiento. Esto se debe a que las comunicaciones y la información que se comparten digitalmente son intermediadas por empresas privadas, las mismas que pueden monitorear el contenido y los metadatos de las comunicaciones. Hay varios actores que pueden estar interesados en dicha información privada. Por un lado, el Estado (o los Estados) como parte de una investigación penal o de inteligencia, pero también organizaciones criminales u otros adversarios podrían estar interesados en acceder y analizar dicha información privada.

En este documento se realiza una descripción de las diversas formas en que se pueden vigilar las comunicaciones en Internet y se muestran ejemplos de herramientas que podrían estar siendo utilizadas por los gobiernos de Honduras, Guatemala, El Salvador y Nicaragua. Se entiende por vigilancia el monitoreo, interceptación, recolección, obtención y análisis de datos usando, preservando, reteniendo o accediendo información que revela o puede llegar a revelar información privada pasada, presente o futura.

El artículo está dividido en tres partes. En la primera parte se describen las distintas formas en las que la comunicación podría ser espiada y quién podría espiarla. Básicamente se analiza la vigilancia en la red de comunicaciones, la vigilancia en el proveedor de servicios de Internet, la inteligencia de fuentes abiertas, la vigilancia con *malware* y el análisis forense. En la segunda parte, se hace una breve descripción de varias herramientas de vigilancia que podrían haber sido adquiridas por los gobiernos centroamericanos de El Salvador, Guatemala, Honduras y Nicaragua. En la tercera parte, se brinda información sobre el uso de estos sistemas en estos cuatro países según lo que se conoce a través información pública. El artículo termina con las conclusiones donde se hace una síntesis de los hallazgos.

Es importante enfatizar que las herramientas de vigilancia podrían ser utilizadas con fines legítimos, sin embargo, sin los controles y garantías adecuadas, su uso podría conllevar abusos de poder. En consecuencia, el objetivo de este documento es visibilizar la existencia de estas herramientas e invitar a la sociedad a conversar sobre el uso de las mismas y las implicaciones que podrían tener para la libertad de las personas.

1. Formas de Vigilancia

La Internet fue diseñada con una naturaleza descentralizada. Fue un proyecto del Departamento de Defensa de Estados Unidos (US DoD) que estableció una red de comunicación que podía resistir desastres. El diseño descentralizado era clave ya que si una pieza del sistema se caía, este seguía funcionado. Este sistema también podía ser utilizado para comunicaciones de punto a punto (peer-to-peer), sin la necesidad de confiar en una sola computadora o empresa. En sus inicios, la conexión a Internet también era descentralizada. No existía una autoridad central sino que si un servidor no funcionaba, los usuarios podrían conectarse de otra manera. La centralización de la Internet comenzó a darse poco a poco con su comercialización[1].

Las grandes proveedoras de acceso a Internet construyeron una infraestructura técnica que es centralizada. Como se detalla en la sección 1.1, esta centralización hace que quienes controlan los cables submarinos por donde viaja la información pueden vigilar la misma. Este tipo de vigilancia, en el caso de la Agencia de Seguridad Nacional de Estados Unidos (NSA por sus siglas en inglés), es denomina UPSTREAM. Involucra el monitoreo, escaneo y recolección de las comunicaciones que viajan por las principales "autopistas" de la Internet. En el caso de la NSA se ha trabajado con empresas proveedoras de acceso a Internet como AT&T[2] para vigilar el gran tráfico de internet que pasa por los cables de fibra óptica de esta empresa en base a la norma legal "702"[3].

En la sección 1.2 se verá que, además de la centralización física por parte de los proveedores de acceso a Internet, también los proveedores pueden poner en riesgo las comunicaciones. Servicios como correo electrónico, chat o voz sobre IP suelen estar provistos por empresas como Google, Microsoft o Facebook. Estas empresas pueden acceder al contenido o metadatos de cierta información, y entregar dicha información al Estado. En este tipo de vigilancia, también conocida como Downstream (o PRISM)[4], los servicios de inteligencia de Estados Unidos obligan a Google, Facebook, y Yahoo a entregar las comunicaciones de quien utiliza las plataformas. Esto incluye comunicaciones entre personas objeto de vigilancia. Las empresas tienen además la prohibición de comunicar a los usuarios que sus datos han sido entregados al gobierno[5].

Más allá de de la vigilancia realizada por agencias como la NSA, es importante notar que proveedores de servicio también son bancos, agencias estatales u otros proveedores de servicios en líneas que almacenan información sobre las personas que los utilizan.

Gran parte de la actividad que es realizada en línea y fuera de línea puede registrarse de manera pública. La vigilancia de fuentes abiertas busca monitorear este tipo de información en Internet, en especial de redes sociales como Facebook, Linkedin, Twitter y otras. Esto es lo que se aborda en la sección 1.3.

En la sección 1.4 se verán las formas en la que dispositivos como teléfonos celulares se pueden convertir en poderosas herramientas de vigilancia con software de empresas como NSO y HackingTeam.

Finalmente, en la sección 1.5 se detallará la información que se podría extraer de un dispositivo celular o una computadora a través de herramientas de análisis forense.

1) Vigilancia del Tráfico de la Red

Internet es en realidad la combinación de muchas computadoras - llamadas servidores - y medios - como cables, antenas y satélites - por donde viajan las comunicaciones. La columna vertebral que conecta a estas redes son los cables submarinos que se pueden ver en la imagen 1. En el caso de América Latina, la mayoría del tráfico de Internet pasa por los Estados Unidos.

1 Tobara, Vince. «The Evolution of the Internet, From Decentralized to Centralized», 28 de marzo de 2018. https://hackernoon.com/the-evolution-of-the-internet-from-decentralized-to-centralized-3e2fa65898f5.

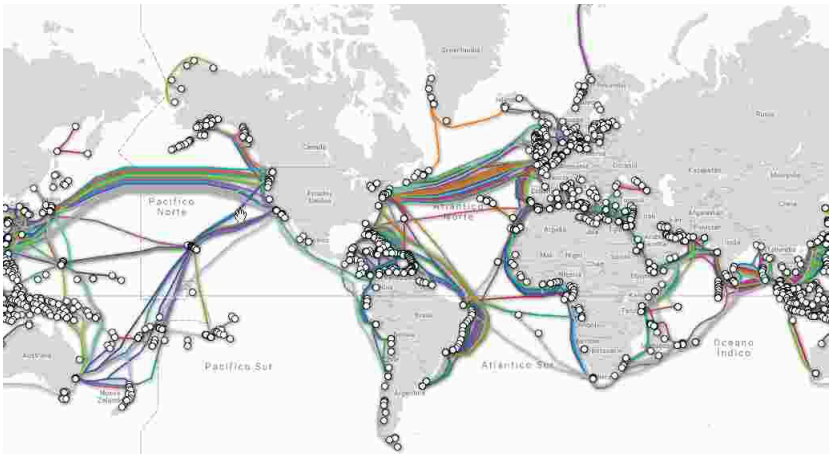
2 Electronic Frontier Foundation. «Upstream vs. PRISM», 2 de octubre de 2017. https://www.eff.org/pages/upstream-prism.

3 Electronic Frontier Foundation. «Decoding 702: What Is Section 702?» Accedido 5 de enero de 2020. https://www.eff.org/702-spying.

4 Eckersley, Dan Auerbach, Jonathan Mayer, and Peter. «What We Need to Know About PRISM». Electronic Frontier Foundation, 12 de junio de 2013. https://www.eff.org/deeplinks/2013/06/what-we-need-to-know-about-prism.

5 Electronic Frontier Foundation. «Upstream vs. PRISM», 2 de octubre de 2017. https://www.eff.org/pages/upstream-prism.

Imagen 1: Cables submarinos en Internet



Fuente: https://www.submarinecablemap.com/

Se sabe por los documentos filtrados por Edward Snowden, que Estados Unidos utiliza el tipo de vigilancia "UPSTREAM"[6] (denominado así por la NSA). Entre los documentos existe una presentación digital donde se menciona el "UPSTREAM" y se describe que recolecta directamente los datos de la infraestructura técnica que detentan las empresas de telecomunicaciones[7]. Es decir, la NSA monitorea, escanea y recolecta las comunicaciones que viajan por cables de fibra óptica por donde pasa Internet.

El esquema centralizado se repite a nivel de los cuatro países centroamericanos del presente estudio, donde proveedores como Claro, Movistar o Tigo se encuentran operando. Si bien, no se evidencia que estas empresas espíen las comunicaciones, existe el riesgo de que esto pueda suceder.

Además las empresas proveedoras de servicio de Internet técnicamente estarían en la capacidad de vigilar las comunicaciones de sus clientes. Una vez más, es importante enfatizar que en este estudio no se evidencia que este sea el caso, pero es importante tomar en cuenta la existencia del riesgo.

Para ilustrar esta idea, pensemos que María quiere acceder a un sitio web. La comunicación no es directa, esta debe pasar por varios dispositivos, conocidos como ruteadores, que se encargan de enviar las comunicaciones a otros ruteadores, y estos a otros, hasta llegar al destino final (ver imagen 2). Se puede pensar en los ruteadores como las oficinas postales que se encargan de enviar cartas a otras oficinas postales hasta llegar a su destino.

Cualquier persona que tenga control sobre los ruteadores o sobre los cables de comunicación tendrá la posibilidad de espiar el tráfico de información que atraviesa por los mismos. Si María accede a sitios web que utilizan el protocolo inseguro HTTP (no cifrado), entonces cualquiera de los ruteadores podrá leer datos y metadatos de las comunicaciones.

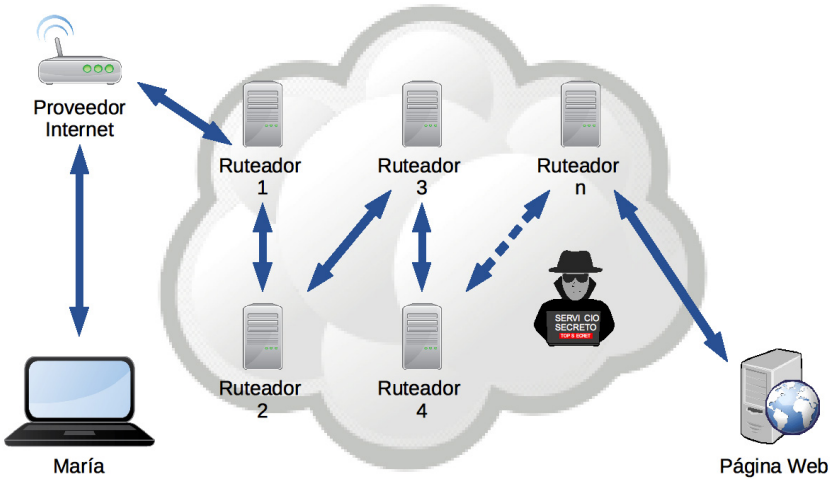
En este sentido, es importante pensar quién podría realizar este tipo de espionaje. La persona u organización que provee una red inalámbrica tendría la capacidad de vigilar la actividad del tráfico de esa red. Este sería el caso, por ejemplo, de los servicios de Internet gratuito en espacios públicos como restaurantes o redes empresariales.

Por otro lado, cuando se accede a internet se debe contratar el servicio de algún proveedor al que se lo conoce como ISP (proveedor de servicio de Internet por sus siglas en inglés). En un ISP trabajan personas y algunas de ellas son responsables de administrar la infraestructura de comunicaciones. Estas personas tienen la capacidad técnica de monitorear las comunicaciones que pasan por sus redes.

6 Just Security. «Unprecedented and Unlawful: The NSA's "Upstream" Surveillance», 19 de septiembre de 2016. https://www.justsecurity.org/33044/unprecedented-unlawful-nsas-upstream-surveillance/.

7 Rumold, Mark. «How EFF's FOIA Litigation Helped Expose the NSA's Domestic Spying Program». Electronic Frontier Foundation, 21 de marzo de 2014. https://www.eff.org/deeplinks/2014/03/sunshine-week-recap-how-effs-foia-litigation-helped-expose-nsas-domestic-spying.

Imagen 2: Ruteadores de Internet



Fuente: Elaboración propia con gráficos de Openclipart

2) Vigilancia desde Proveedores de Servicio

Cuando María envía un mensaje a José a través de WhatsApp, la información viaja primero a los servidores de WhatsApp; cuando le envía un correo a través de Gmail, este viaja por los servidores de Google. En el caso de Gmail, Google puede saber que María y José se están comunicando e incluso el contenido de los correos. Con WhatsApp o Facebook (dueños de WhatsApp) pueden saber que María y José se comunican, pero no el contenido de los chats[8]. Algo similar sucede con otros servicios como sitios de noticias, banca en línea, tarjetas de crédito y débito, servicios del Estado y otros pueden recolectar información de la actividad de las personas.

En el caso de Estados Unidos se sabe que empresas como Google, Microsoft, Facebook, Apple y otras dan acceso a la información recolectada de sus usuarias y usuarios a través del programa "*Downstream*" o como lo denomina la NSA, PRISM.

En la imagen 3 se muestra una diapositiva de un documento de 2013 del gobierno de Estados Unidos publicado por Edward Snowden. En la misma se puede ver que empresas participaban en PRISM[9] y el tipo de información que recolectan. Además, es posible que en la actualidad el número de empresas haya aumentado.

> "En la vigilancia "downstream", la comunidad de inteligencia busca comunicaciones que son hacia o desde "selectores" o identificadores que se cree que están vinculados a objetivos (Targets) de inteligencia extranjeros. Los selectores pueden ser cosas específicas como direcciones de correo electrónico, pero también pueden ser datos mucho más amplios." (...)
>
> "En la vigilancia 'downstream', las agencias de inteligencia de EE. UU. van directamente a compañías como Google, Facebook y Yahoo y obligan a las compañías a entregar las comunicaciones hacia y desde los selectores identificados, incluidas las comunicaciones entre los targets y las personas estadounidenses. A las compañías se les prohíbe decir a sus usuarios que sus datos han sido entregados al gobierno."[10]

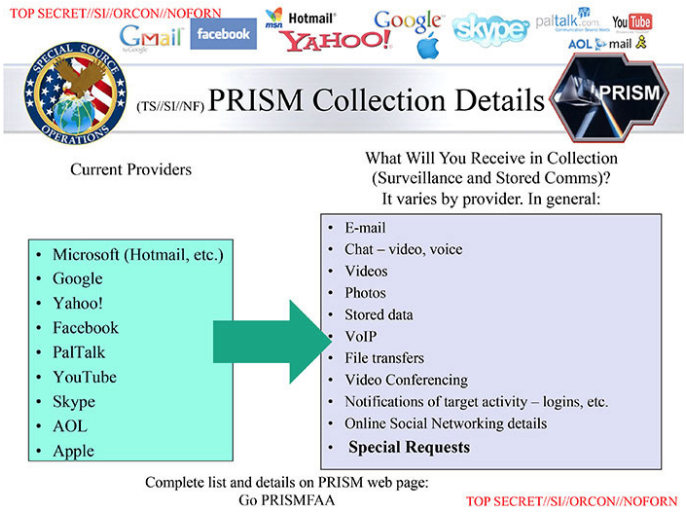
Asimismo, es importante considerar que si una persona no tiene nacionalidad de Estados Unidos y vive fuera de este país, los Estados Unidos pueden vigilar legalmente su información a través de las agencias como la NSA, CIA o FBI, ya que la protección constitucional vigente en USA no se extiende a personas no estadounidenses.

8 Esto no es completamente cierto ya que, si bien los chats de WhatsApp son cifrados, estos también se suelen respaldar sin cifrar en servidores de WhatsApp podría leerlos. Ver: Gebhart, Bill Budington and Gennie. «Where WhatsApp Went Wrong: EFF's Four Biggest Security Concerns». Electronic Frontier Foundation, 13 de octubre de 2016. https://www.eff.org/deeplinks/2016/10/where-whatsapp-went-wrong-effs-four-biggest-security-concerns.

9 Electronic Frontier Foundation. «Upstream vs. PRISM», 2 de octubre de 2017. https://www.eff.org/pages/upstream-prism.

10 Electronic Frontier Foundation. «Upstream vs. PRISM», 2 de octubre de 2017. https://www.eff.org/pages/upstream-prism.

Imagen 3: Empresas participantes en el programa PRISM



Fuente: https://edwardsnowden.com

No se han encontrado evidencias sobre un programa similar a "downstream" en los países de la región materia del estudio. Sin embargo, es importante recordar que los gobiernos pueden realizar solicitud de información a empresas como Google, Facebook, Twitter y otras conforme a la legislación de cada país y los tratados de asistencia mutua legal. Normalmente estas solicitudes deberán seguir los procedimientos determinados por el marco legal vigente y los tratados internacionales.

Estas empresas (Facebook[11], Google[12] y Twitter[13]) publican semestralmente las solicitudes de información realizadas por gobiernos a nivel mundial. En la siguiente tabla se puede ver las solicitudes realizadas por los países analizados en este informe desde el primer semestre de 2016 hasta el primer semestre 2018. La columna marcada con S muestra el número de solicitudes, mientras que la columna marcada con U el número de cuentas de usuarios afectados.

11 «Requests For User Data», accedido 5 de marzo de 2019, https://transparency.facebook.com/government-data-requests/.

2 «Solicitudes de información sobre usuarios – Informe de transparencia de Google», accedido 5 de marzo de 2019, https://transparencyreport.google.com/user-data/overview.

13«Information Requests», accedido 5 de marzo de 2019, https://transparency.twitter.com/en/information-requests.html.

Tabla 1

Solicitudes de información realizadas por gobiernos de Guatemala, El Salvador, Honduras y Nicaragua a Facebook, Google, Twitter (2016-2018)

Facebook										
País	2016				2017				2018	
	1er semestre		2do semestre		1er semestre		2do semestre		1er semestre	
	S	U	S	U	S	U	S	U	S	U
El Salvador	6	8	3	3	6	18	16	23	23	35
Guatemala	26	45	34	82	66	738	82	208	169	338
Honduras	2	2	0	0	2	2	0	0	0	0
Nicaragua	-	-	-	-	-	-	-	-	-	-
Google										
País	2016				2017				2018	
	1er semestre		2do semestre		1er semestre		2do semestre		1er semestre	
	S	U	S	U	S	U	S	U	S	U
El Salvador	2	2	1	1	1	1	3	3	0	0
Guatemala	0	0	2	2	0	0	0	0	6	10
Honduras	-	-	-	-	-	-	-	-	-	-
Nicaragua	-	-	-	-	-	-	-	-	-	-
Twitter										
País	2016				2017				2018	
	1er semestre		2do semestre		1er semestre		2do semestre		1er semestre	
	S	U	S	U	S	U	S	U	S	U
El Salvador	4	4	0	0	0	0	4	4	4	11
Guatemala	0	0	5	5	2	2	1	1	1	1
Honduras	0	0	0	0	1	1	0	0	0	0
Nicaragua	-	-	-	-	-	-	-	-	-	-

Fuente: Elaboración propia a partir de informes de las empresas

Si bien no se conoce el motivo de estas solicitudes, se muestra que, salvo Nicaragua, los gobiernos de la región tienen la capacidad de solicitar información a empresas extranjeras, aunque por este medio lo hacen de manera poco frecuente.

Por otro lado, es importante tomar en cuenta que los servicios en línea provistos por estas empresas no son los únicos que se pueden utilizar para recolectar información de las personas de un país. Las empresas de telefonía o empresas proveedoras de Internet también puede realizar vigilancia de las comunicaciones a nivel nacional. De forma adicional, el Estado maneja varios sistemas[14] con información de las personas, normalmente asociados al documento de identidad. Así, el documento de identidad podría ser utilizado para relacionar información entre varios sistemas estatales.

Además, bancos, supermercados y otras empresas también recolectan información sobre las personas que, sin los controles necesarios, podría ser espiada.

14 Cope, Saira Hussain and Sophia. «DEEP DIVE: CBP's Social Media Surveillance Poses Risks to Free Speech and Privacy Rights». Electronic Frontier Foundation, 5 de agosto de 2019. https://www.eff.org/deeplinks/2019/08/deep-dive-cbps-social-media-surveillance-poses-risks-free-speech-and-privacy.

3) Inteligencia de Fuentes Abiertas

Como ya se señaló, la actividad que realizan las personas en Internet deja huellas. Las redes sociales son utilizadas para compartir momentos con amistades, fotos, proyectos, causas políticas, etcétera. Además de las redes sociales, personas defensoras de derechos humanos también tienen presencia en blogs o han aparecido en algún medio digital. Esa información queda almacenada y es accesible en el futuro por terceros.

Facebook, Twitter o el uso de redes sociales plantea una disyuntiva con respecto a la seguridad. Por un lado, las redes sociales pueden ser una herramienta útil para manifestar opiniones políticas o incluso organizar manifestaciones. Es también el espacio donde muchas personas, incluyendo activistas, comparten parte de su vida privada. Sin embargo, esto es un riesgo, ya que, por ejemplo, un Estado que abuse en contra de los derechos humanos de las personas podría utilizar la información publicada en redes sociales para amedrentar a disidentes políticos.

En síntesis, cualquier persona con tiempo y ganas puede investigar la actividad en línea de otra persona a través de buscadores como el de Google o los buscadores propios de cada red social u herramientas más sofisticadas que permiten al Estado y otros actores monitorear información que está disponible públicamente.

4) Espionaje con *Malware*

Las computadoras portátiles de hoy en día cuentan con micrófono y cámara. Los teléfonos celulares, además de la cámara y el micrófono, tienen GPS y se encuentran conectados constantemente a Internet. Si estos dispositivos llegaran a ser controlados de forma remota pueden ser poderosas herramientas de vigilancia.

Para tomar control remoto de los dispositivos es necesario en su mayoría de casos explotar una vulnerabilidad en el software, para así poder instalar un software malicioso conocido como *malware*. Con *malware* instalado es posible tomar control sobre el teléfono de un objetivo de vigilancia de manera remota y en tiempo real. Esto quiere decir que toda la actividad realizada en el mismo puede ser vigilada: mensajes de texto, chats de WhatsApp o Signal, fotos, etcétera. Además, es posible prender el micrófono y la cámara para espiar en tiempo real lo que está sucediendo alrededor del dispositivo o utilizar la información de ubicación y así saber en que lugar y a que hora se encuentra el objetivo de vigilancia.

A diferencia de las herramientas vistas hasta ahora, para el uso de *malware* el adversario debe tener la capacidad de instalar el software en el dispositivo de la víctima. Esto se puede hacer de varias formas. Una de las más frecuentes es el envío de mensajes de texto con enlaces a páginas web que intentan engañar a la persona para hacer click e instalar el software malicioso. Otra técnica podría ser el envío un correo electrónico con un archivo que explota una vulnerabilidad al momento que se instala el archivo malicioso.

5) Análisis Forense

Las herramientas de análisis forense son utilizadas por policías de todo el mundo para resolver casos legales. La información almacenada en un disco duro, una memoria USB, un teléfono móvil u otro medio puede servir de evidencia en un caso legal. Es importante considerar que las herramientas forenses tienen la capacidad de identificar incluso los archivos eliminados de los dispositivos analizados. Es más, los archivos eliminados constituyen una de las primeras pistas que un investigador forense utilizará.

A diferencia de las otras modalidades de vigilancia, para el análisis forense es necesario tener acceso físico a un dispositivo. Por otro lado, al realizar un análisis forense sobre un teléfono celular, por ejemplo, además de la información almacenada en el mismo se puede acceder a la información en la “nube” de las cuentas de Internet asociadas a estos teléfonos. Esto es algo de lo que presumen las herramientas modernas de análisis forense. Es importante notar que las herramientas forenses pueden ser utilizadas con fines legítimos, pero sin los controles necesarios, las mismas podrían prestarse para abusos.

2. Herramientas de Vigilancia

En la sección 1 se abordaron las formas de vigilancia que podrían ser utilizadas por el Estado. En esta sección, salvo el espionaje en el ámbito de proveedor de servicios, se verá como empresas que ofertan tecnología podrían explotar estos modelos de amenaza.

En la sección 2.1 se verán las empresas que ofertan productos en dos o más modelos de amenaza descritos en la sección 1; en la sección 2.2 se verán las herramientas de vigilancia para red; en la sección 2.3 las empresas que ofertan herramientas para inteligencia de fuentes abiertas; en la sección 2.4 herramientas de *malware*; y en la sección 2.5 se verán las herramientas de análisis forense. Por último, en la sección 2.6 se verá la herramienta IBM I2 Analyst's Notebook para análisis de información.

1) Recolección de Datos de dos o más Formas

Empresas como Penlink y Verint se enfocan en más de un modelo de amenaza para ofertar sus productos.

1. Penlink

Penlink es un software de vigilancia que permite recolectar y analizar información de redes sociales, interceptar llamadas telefónicas y georreferenciar dispositivos móviles. Tiene algunos productos como PLX, Pen-Proxy, Netviz, Innovation[15].

- **PLX** es un producto integrado que permite recolectar y analizar información. La recolección se puede hacer en tiempo real e incluye herramientas para investigar actividad en redes sociales e intervenir comunicaciones.
- **PenProxy** permite vigilar redes de telefonía (y comunicaciones) en tiempo real. Dice generar alertas de llamadas telefónicas, SMS o correos electrónicos. Puede cruzar información con otras bases de datos.
- **Netviz** permite analizar información y formar gráficos. Ofrece un servicio en línea con un costo US$ 39.99 por la versión básica y US$ 99.99 por la versión completa. Además, cuenta con una versión gratuita por 60 días.
- **Innovation** parece no ser un producto, sino una serie de servicios, como el uso de "cloud" para analizar información, *big data* y *machine learning*.

2. Verint

Verint es una empresa que ofrece diversas herramientas de vigilancia digital que incluyen además videovigilancia y reconocimiento facial. Varias de sus herramientas se caracterizan por tener capacidades de vigilancia masiva. Es decir, como se verá a continuación, permiten espiar de forma masiva a un grupo de personas.

En su sitio web muestran algunas de las características de los productos disponibles. Uno de ellos se llama "Inteligencia en Redes" (Network Intelligence). En la descripción de esta herramienta dicen poder recolectar prácticamente todo el tráfico de una red a cualquier escala. Además de interceptar el tráfico, lo puede analizar en tiempo real o de manera retrospectiva. Asimismo, dice, por ejemplo, tener la capacidad de detectar patrones de comportamiento sospechoso[16].

"Red de Inteligencia" (Web Intelligence) es otro producto ofrecido por esta empresa. Esta herramienta se encarga de analizar la información publicada en Internet a través de redes sociales. La herramienta dice tener la capacidad de analizar la internet pública, así como la red profunda y redes oscuras[17]. Se entiende que es una herramienta poderosa para la inteligencia de fuentes abiertas.

---

15 «PenLink | Penlink.Com», accedido 16 de enero de 2019, https://www.penlink.com/. En el sitio se detalla la funcionalidad de cada uno de los productos.

16 «Network Intelligence», Verint CIS, accedido 15 de febrero de 2019, https://cis.verint.com/product/network-intelligence/.

17 «Web Intelligence - Verint CIS», accedido 14 de febrero de 2019, https://cis.verint.com/product/web-intelligence/.

Los productos de vigilancia tecnológica ofrecidos por esta empresa van más allá de las comunicaciones. En este sentido, cuenta con soluciones para videovigilancia que incluyen cámaras, sistemas de análisis y software de reconocimiento facial. Concretamente, es FaceDetect[18] el producto de reconocimiento facial ofertado por esta empresa. Entre las características que presumen tener, señalan contar con el mayor porcentaje de resultados positivos y el menor de falsos positivos. Asimismo, afirman tener la capacidad de detectar personas incluso de imágenes de baja resolución, hasta de 45 x 45 píxeles, y dicen poder trabajar con bases de datos de 200 millones de fotos.

Si el sistema puede manejar bases de datos con tantos rostros, entonces puede funcionar como un sistema de vigilancia masiva innecesaria y desproporcionada. El uso de reconocimiento facial se podría justificar, de existir una normativa que la autorice, sea proporcional y mediante autorización judicial. Sin embargo, presumir que se puede manejar bases de datos de 200 millones de personas implicaría una importante interferencia con el derecho a la privacidad.

Todas estas herramientas, sumadas con otras fuentes de información, pueden ser analizadas con el sistema OMNIX[19]. De esta manera, la información tomada desde el sistema de monitoreo en redes, se suma a la del sistema de monitoreo en Internet, más la información de videovigilancia. Esto permitiría cruzar toda la información de los objetivos de vigilancia.

Cabe destacar que Verint, como empresa, tiene dos divisiones. La primera es la que ofrece las soluciones de vigilancia mencionadas en esta sección. La segunda división ofrece servicios para mejorar la relación entre clientes y empresas. Se puede leer en la página frases como "¿Necesita una arquitectura moderna para monetizar sus datos? Nuestras soluciones capturan datos de clientes y de la fuerza laboral que se pueden compartir fácilmente en su empresa."[20] En este análisis se ha visto el funcionamiento de Verint dedicada a la ciberinteligencia, pero no se ha investigado sobre la otra área de esta empresa.

2) Recolección de Datos en la Red

1. Bluecoat

Bluecoat es un sistema tradicionalmente utilizado por corporaciones para optimizar el uso de la red. Por ejemplo, los bancos lo podrían usar para limitar el acceso a Internet y de esta forma mejorar la seguridad. Asimismo, organizaciones públicas y privadas lo usarían para optimizar el uso de los recursos de la red. Se podría, por ejemplo, usar BlueCoat para disminuir el consumo de ancho de banda limitando el acceso a sitios como YouTube.

La tecnología que utiliza una empresa para compartir el acceso a Internet es similar a la que utilizan los proveedores de Internet para distribuir este recurso al nivel de un país. Un proveedor de Internet podría instalar alguno de los productos de BlueCoat y de esta manera analizar el tráfico en la red de todos sus clientes. Un Estado podría hacer lo mismo en las conexiones con cables submarinos y analizar el tráfico de la red de todos sus abonados. La información recolectada luego puede ser analizada.

La posibilidad de bloquear sitios web en un banco, se convierte en censura cuando es aplicado por un Estado o proveedor de Internet sobre el contenido disponible públicamente. Para poder optimizar el uso de ancho de banda, es necesario analizar y clasificar el tráfico. Así, para que el proveedor de Internet pueda priorizar el tráfico para ver videos, debe poder analizarlo y clasificarlo poniendo en riesgo la privacidad de sus usuarios.

2. Circles

Se investigó la empresa Circles debido a que la misma aparece en una investigación del medio guatemalteco "Nuestro Diario". Dicha investigación describe la herramienta[21] de la siguiente manera:

---

18 Verint, «FaceDetect - Facial Recognition for de Real World», 2018, https://cis.verint.com/wp-content/uploads/2018/03/Verint-FaceDetect-March-2018-Final.pdf.

19 «OMNIX Intelligence Fusion Center - Verint CIS», accedido 15 de febrero de 2019, https://cis.verint.com/product/intelligence-fusion-center/.

20 Verint, «Soluciones de optimización del compromiso con el cliente | Verint Systems», page, 10-CES-Home, accedido 18 de febrero de 2019, https://es.verint.com/engagement/index.html.

21 Sas, Luis Angel, «Espionaje ilegal del Gobierno: Aquí está la investigación de Nuestro Diario (Parte I)», Nómada, Guatemala., 7 de agosto de 2018, https://nomada.gt/pais/la-corrupcion-no-es-normal/espionaje-ilegal-del-gobierno-aqui-esta-la-investigacion-de-nuestro-diario-parte-i/.

Intercepta llamadas, tráfico de Internet, desencripta mensajes. Utiliza un dispositivo que se hace pasar por antena, todo desde una compañía en Bulgaria.

No existe mucha información en Internet referente a Circles, más allá de una investigación del portal búlgaro de periodismo investigativo Bibl.bg[22]. Esta investigación describe a Circles como una empresa que ofrece servicio de interceptación de llamadas de telefonía celular en tiempo real. Para poder ofrecer este servicio a nivel global, Circles se registró como operadora móvil virtual y obtuvo llaves de cifrado para poder interactuar con las empresas Magyar Telekom de Hungría, Telecom Italia y Cogent de Estados Unidos. De esta manera tuvieron acceso al tráfico de la red SS7, que es la que permite la comunicación telefónica a nivel mundial. Una vez dentro de la red, explica la investigación, Circles podría interceptar llamadas telefónicas o incluso la ubicación de teléfonos a nivel global.

El sitio web de Circles ya no está disponible, es probable que la empresa ya no opere o que haya cambiado de nombre. En el archivo histórico de Internet se constató la existencia de la página con muy poca información. Concretamente, hasta diciembre de 2014 contaban con una página web con tan solo un correo electrónico de contacto[23]. Como ya se ha señado, la última vez que la página fue archivada contenía muy poca información, pero buscaba posicionar que la información es una herramienta poderosa. De hecho, señalaba que no se trata de quién tiene las armas, sino quién controla la información[24].

3) Inteligencia de Fuentes Abiertas

1. Conceptus

La agencia SIBAT del ministerio de defensa de Israel tiene como propósito la colaboración en seguridad de gobierno a gobierno[25]. Entre sus actividades publica un catálogo de productos enfocados en seguridad. En la edición 2018-2019[26] de dicho catálogo se describe a Conceptus como un sistema de inteligencia para la web y redes sociales con las siguientes características:

- Permite manejar cuentas en redes sociales (Avatares).
- Se usa para inteligencia humana (HUMINT), es decir inteligencia hacia personas.
- Tiene soporte multidioma.
- Tiene servicios de inteligencia que permiten monitorizar internet público y la red oscura (darknet).
- Monitoreo de transacciones de Bitcoin y las identidades detrás de las mismas.

4) Malware

1. Pegasus / NSO

Pegasus es un *malware* que permite tomar control remoto de computadoras o teléfonos móviles. Esto implica encender la cámara del teléfono o el micrófono, acceder a archivos, chats, etcétera. Un informe publicado por Citizenlab en 2016 demostró que México era, con mucha diferencia, el país con mayor infraestructura dedicada a servidores de Pegasus[27].

En este sentido, otro reporte realizado por las organizaciones R3D, Article 19 y SocialTIC muestra intentos de ataques realizados contra personas defensoras de derechos humanos y periodistas. Para ello, se empleó una

22 «Bulgarian Company – Global Innovator in Wiretapping», Text, Bivol.Bg (blog), 15 de diciembre de 2015, https://bivol.bg/en/bulgarian-company-global-innovator-in-wiretapping.html.

23 «circles», 16 de diciembre de 2014, https://web.archive.org/web/20141216224900/http://circles.bz/.

24 «Circles», 11 de mayo de 2018, https://web.archive.org/web/20180511064936/http://www.circles.bz/.

25 «SIBAT | Opening Doors», accedido 30 de enero de 2019, http://www.sibat.mod.gov.il/OurServices/Pages/OpeningDoors.aspx.

26 The Israel Ministry of Defense, SIBAT - International Defense Cooperation. «Israel Homeland & Cyber Defense Directory 2018-19», 2018, pág 58, http://www.sibat.mod.gov.il/Industries/directory/Documents/Sibatdir-HLS-en2018-19.pdf.

27 Marczak, Bill y Scott-Railton, John, *The Million Dollar Dissident: NSO Group's iPhone Zero-Days used against a UAE Human Rights Defender,* 2016, https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/.

estrategia combinada de envío de mensajes de texto con enlaces hacia sitios que podrían implantar el software malicioso a las víctimas. Entre las víctimas se encuentran miembros del Centro de Derechos Humanos Miguel Agustín Pro Juárez, que denunciaron el caso de los 43 estudiantes desaparecidos de Ayotzinapa. También se constató el intentó de espiar a la periodista Carmen Aristegui y a su hijo, menor de edad en ese momento[28].

2. Galileo / HackingTeam

Galileo es el software distribuido por la empresa Italiana Hacking Team. Entre otras cosas, permite tomar control remoto de computadoras y celulares para acceder a la cámara, el micrófono, los chats o la ubicación. Esta empresa fue expuesta ante la opinión pública por primera vez, con la revelación de los archivos "Spyfiles" de Wikileaks[29] que involucraron a decenas de empresas en diciembre del año 2011.

Posteriormente, el 5 de julio de 2015, la empresa fue vulnerada de manera electrónica y se hicieron públicos 400 gigas de información que incluían correos electrónicos, facturas o código fuente, entre otros archivos. La organización Derechos Digitales realizó una investigación sobre estos documentos que evidenció que 7 países de América Latina compraron el software de esta empresa. Además, otros 5 países mantuvieron negociaciones[30]. En el caso de Centroamérica - como se verá en la sección 3 de este documento - Honduras pertenece al primer grupo, mientras que Guatemala al segundo.

A pesar del escándalo, la página web de la empresa sigue funcionando y en la misma presume de sus capacidades. De hecho, en un video promocional explica como este sistema puede ser utilizado para evadir el cifrado de las comunicaciones o incluso para acceder a información que no se ha enviado. Asimismo, señalan que el sistema puede monitorear a cientos de miles de personas desde un solo lugar[31].

5) Análisis Forense

Las herramientas de software forense son utilizadas por agencias policiales a nivel mundial. Las mismas deberían ser utilizadas con fines legítimos, pero a falta de controles adecuados, también podrí para abusos.

1. Cellebrite

Cellebrite es una empresa de análisis forense para teléfonos celulares. Tuvo sus inicios en 1999 como una aplicación que permitía exportar contactos de un teléfono a otro, una tarea complicada en esa época. Con el tiempo la aplicación generó interés de agencias policiales y Cellebrite vio el potencial de entrar el mundo del software de análisis forense. En 2016, pocos meses después de que el FBI encontró la manera de descifrar un teléfono IPhone con el sistema operativo IOS 9, Cellebrite anunció que ellos también sabían como hacerlo, según reportó el diario digital The Intercept[32].

En su categoría de software forense, Cellebrite puede extraer información de un teléfono. Esto incluye también la información que haya sido eliminada. Según The Intercept, Cellebrite se diferencia de sus competidores por la capacidad de poder extraer información de casi cualquier teléfono celular. En este caso, la empresa está trabajando para poder acceder a teléfonos bloqueados. Existe una gran diferencia entre la capacidad de realizar análisis forenses de teléfonos bloqueados y desbloqueados porque en el primer caso implica derrotar o eludir los sistemas de seguridad del teléfono.

La información contenida en un teléfono celular incluye historial de llamadas, mensajes de texto o historial de localización. También contiene otro tipo de información, que varia en cada caso, dependiendo las aplicaciones instaladas. Además, como ya se ha señalado, estos dispositivos suelen estar conectados a cuentas de redes sociales, correo electrónico, etcétera. En consecuencia, a través de herramientas como Cellebrite se podría extraer ese tipo de información.

---

28 R3D, Article 19, y SocialTIC, *Gobierno Espía*, 2017, https://r3d.mx/gobiernoespia.

29 Wikileaks, «WikiLeaks - Releases», accedido 7 de marzo de 2019, https://wikileaks.org/spyfiles/releases/.

30 Pérez de Acha, Gisela, «Hacking Team Malware para la Vigilancia en América Latina» (Derechos Digitales, marzo de 2016), https://www.derechosdigitales.org/wp-content/uploads/malware-para-la-vigilancia.pdf.

31 «HackingTeam», accedido 7 de marzo de 2019, http://hackingteam.it/solutions.html.

32 Kim Zetter, «When the FBI Has a Phone It Can't Crack, It Calls These Israeli Hackers», The Intercept (blog), 31 de octubre de 2016, https://theintercept.com/2016/10/31/fbis-go-hackers/.

2. Magnet Axiom

Magnet Axiom es una familia de software forense que permite recuperar información, incluso la borrada, de teléfonos móviles, computadoras y de la nube. Los sistemas de Magnet Axiom, luego de recuperar la información, tienen sofisticadas herramientas de análisis de datos, que incluyen inteligencia artificial, para buscar conexiones entre la información recuperada de teléfonos, computadoras e información en la nube[33].

3. Encase

Encase es un conjunto de herramientas de software y hardware para investigaciones policiales. Al igual que otros sistemas de análisis forense, permite copiar el contenido íntegro de los dispositivos de almacenamiento, esto incluye incluso los archivos forenses. Dicen tener, además, la capacidad de descifrar dispositivos de almacenamiento, pero no explican como[34].

Encase ha sido tradicionalmente conocido por su capacidad para hacer copias y análisis forense de discos duros. Sin embargo, ofrece también opciones para dispositivos móviles como teléfonos, tabletas y otros[35].

6) Análisis de Información

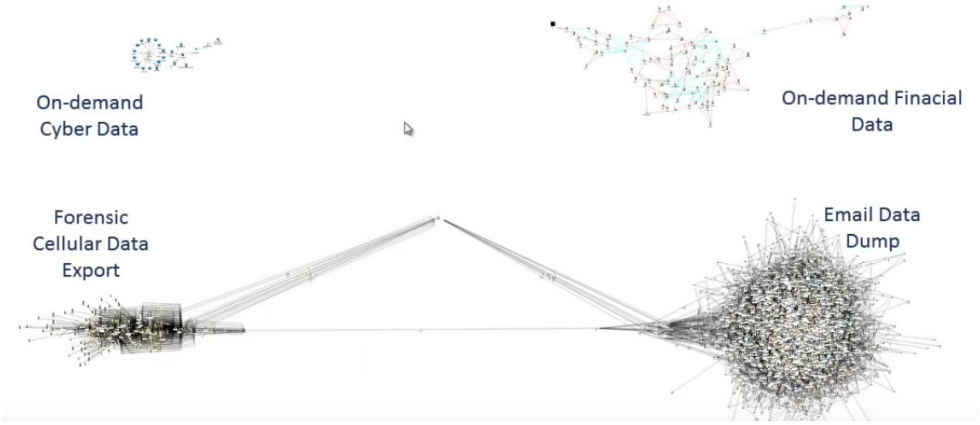
La información recolectada por los medios antes mencionados puede llegar a ser mucha. Por lo tanto, es necesario contar con herramientas para analizar dicha información. Existen herramientas especializadas para el análisis de este tipo de información, como es el caso de IBM I2 Analyst´s Notebook.

1. IBM I2 Analyst's Notebook

IBM I2 Analyst's Notebook (IBM I2 en adelante) es un sistema de análisis de información que existe desde 1980 y es utilizado por agencias de inteligencia a nivel mundial. En 2011 fue adquirido por IBM, quien ahora controla el sistema.

IBM I2 se puede adquirir, según su página web,[36] a partir de US$9.060 por usuario. Esta herramienta permite realizar análisis avanzado de información de varias fuentes. Concretamente, puede cargar datos de hojas de cálculo, archivos de correo electrónico o información recolectada por herramientas como las mencionadas en los apartados previos. En la imagen 4 se ve una captura de pantalla de un video promocional de IBM donde muestra un ejemplo de cómo relaciona "cyber datos en demanda", información forense de celular, información financiera y un archivo de correo electrónico.

Imagen 4: Captura de pantalla video IBM I2



Fuente: https://www.ibm.com/us-en/marketplace/analysts-notebook

33 «Magnet AXIOM», *Magnet Forensics Inc.* (blog), accedido 6 de febrero de 2019, https://www.magnetforensics.com/magnet-axiom/.

34 «EnCase Forensic Software - Top Digital Forensics & Investigations Solution», accedido 6 de febrero de 2019, https://www.guidance-software.com/encase-forensic.

35 «EnCase Mobile Investigator - Mobile Forensics Investigation Solution», accedido 6 de febrero de 2019, https://www.guidancesoft-ware.com/encase-mobile-investigator?

36 «IBM i2 Analyst's Notebook - Overview - United States», accedido 30 de enero de 2019, https://www.ibm.com/us-en/marketplace/analysts-notebook.

IBM I2 funciona como una herramienta complementaria a las vistas hasta ahora. En este sentido, los "cyber datos en demanda" se podrían conseguir a través de espionaje en la red o malware en un teléfono. La información financiera se podría solicitar al proveedor del servicio, por ejemplo, un banco. De manera similar, se podrían conseguir los archivos de correos electrónicos. Además, mediante herramientas forenses para celulares se podría cargar la información de un teléfono confiscado.

3. Uso de Herramientas por países

En esta sección se hará una descripción de lo que se conoce sobre la adquisición y uso de las herramientas antes mencionadas en la región. En la siguiente tabla se muestra un resumen de los hallazgos encontrados, mientras que más adelante se verá el detalle de cada país, aportando el sustento de la información contenida en la tabla.

Tabla 2

Empresa	Recolección de Información				Análisis de Información	Países	
	Red	Internet / OSINT	Malware	Forense		Indicios	Verificado
Penlink	X	X			X	GT,SV	
Verint	X	X			X	HN,SV,NI	
Bluecoat	X						GT,NI
Circles	X					GT	
Conceptus		X				GT	
NSO			X			GT	
HackingTeam			X			GT	HN
Cellebrite				X	X		SV,GT
Encase				X	X		SV,HN,NI
Magnet				X	X		GT
IBM I2					X		GT

Fuente: elaboración propia.

1) El Salvador

1. Penlink

Un documento sobre la planificación anual de la Escuela de Capacitación Fiscal de la Fiscalía General de la República, muestra que en abril de 2016 estaba disponible la "CERTIFICACION PARA ADMINISTRADORES AVANZADOS EN SISTEMA INFORMÁTICO PEN-LINK". Dicha capacitación debió haberse realizado en Estados Unidos.[37] Si bien no se ha encontrado evidencia de contratos de compras del software, a partir del hecho de que se promocione la capacitación se puede inferir que podría estar siendo utilizando.

2. IBM I2

Según las memorias laborales de la Fiscalía de El Salvador del año 2013-2014, en diciembre de 2013 se dictó una jornada de capacitación de cinco días sobre el uso de esta herramienta de IBM. La actividad fue organizada por la empresa BACTO, distribuidora de productos de IBM en Centroamérica[38].

3. Verint

En el caso de El Salvador también hay indicios de la presencia de Verint. Según el informe de labores de Tania Molina Avalos, que se desempeñaba como jefa de gabinete de Cancillería, en el primer trimestre de 2011 se tuvo una visita oficial a Israel. Durante dicha visita se realizó una "Visita a la Compañía Verint (soluciones tecnológicas de seguridad)."[39]

37 «Programacion-abril-2016.pdf», accedido 17 de enero de 2019, http://escuela.fgr.gob.sv/wp-content/uploads/programacion-cursos/Programacion-abril-2016.pdf.

38 «Fiscal General inaugura curso Especializado sobre Nuevas Técnicas de Investigación», accedido 21 de enero de 2019, http://www.fiscalia.gob.sv/wp-content/uploads/memoria-2013-2014/files/assets/basic-html/page129.html.

39 Molina Avalos, Tania. «Hoja de Vida - Tania Molina Avalos», 2012. https://www.transparencia.gob.sv/institutions/rree/documents/242354/download.

En diciembre de ese mismo año Verint inició el registro de marca en El Salvador, como consta en el registro del Diario Oficial de ese mes. Dice, entre otras cosas, que se registra la marca para:

> Hardware y software de computadora en el campo de las telecomunicaciones, seguridad digital y vigilancia, seguridad inteligencia, redes y multimedia de computadoras y telecomunicaciones, para monitoreo, adquisición, grabación, análisis y almacenamiento de voz, fax, video, internet, datos y pantallas de computadora o su uso desde múltiples canales de telecomunicaciones, para su uso en la seguridad pública, servicios financieros, ventas al por menor, cuidado de la salud, telecomunicaciones, aplicación de la ley, gobierno, transporte, utilidades (localidades gubernamentales), y sectores de infraestructura crítica, y manuales de instrucción, todo lo anterior vendido como una sola unidad. Software de computadora para monitoreo, grabación y análisis de interacciones de clientes a través de varios medios y mecanismos de comunicación para propósitos de optimizar a los empleados en operaciones de servicio al cliente en centros de contacto, sucursales, y entornos de oficina; software de computadoras para propósitos de programación, cuadros de mandos, retro alimentación, encuestas, administración de personal, entrenamiento, aprendizaje electrónico, gestión del desempeño, capacitación y representación de informes sobre los empleados, software de computadoras para grabación, búsqueda o análisis de discursos estructurados o no estructurados, textos o comunicaciones de datos para propósitos de análisis de servicios, productos, experiencias, opiniones, comportamiento o tendencias de otros.[40]

4. Encase y Cellebrite

La Corte de Cuentas de la República de El Salvador realizó una auditoría a la Fiscalía General de la República correspondiente al periodo del 1 de febrero al 31 de julio de 2017.[41] El informe de auditoría evidencia que se actualizaron varias licencias vinculadas a Cellebrite. Se trataba de licencias para la herramienta UFED ($21 205.85) y licencias UFED Cloud ($10 043.19). Además, en el caso de Encase compraron 30 horas de capacitación en línea para el uso de este sistema ($2 976.42).

Se ha logrado identificar además, el uso de herramientas como Cellebrite en casos judicializados en 2015[42], 2016[43] y otros. En el 2016, se combinaron tecnologías como las herramientas de Cellebrite con I2 Analytic's Notebook de IBM:

> Equipo utilizado: El aparato denominado UFED (Universal Forensic Extraction Device) versión 2, del sistema CelleBrite, para obtener los datos almacenados en el teléfono, el software denominado i2 Analyst's Notebook 8.0, para realizar el cruce de llamadas telefónicas y números en común[44]

2) Guatemala

1. Bluecoat

Una investigación realizada por el "Citizen Lab" de la Universidad de Toronto en el año 2013 descubrió que 83 países, ejecutaban los productos PacketShaper and ProxySG de BlueCoat. En el caso de Centro América se encontraron 4 servidores con PacketShapper en Guatemala y 9 en Nicaragua, según los datos aportados por la investigación.[45]

---

40 «DIARIO OFICIAL», 21 de diciembre de 2011, 131, https://www.diariooficial.gob.sv/diarios/do-2011/12-diciembre/21-12-2011.pdf.

41 «Informe de Examen Especial al Presupuesto Extraordinario de Seguridad Pública, Ejecutado Por La Fiscalía General De La República, por el Periodo del 1 de Febrero al 31 de Julio De 2017» (Corte de Cuentas de la República, 6 de octubre de 2017), http://www.cortedecuentas.gob.sv/index.php/en/resultado-del-proceso-de-fiscalizacion/informes-finales-de-auditoria/direccion-de-auditoria-1/2017-dea01?download=7478:informe-de-examen-especial-al-presupuesto-extraordinario-de-seguridad-publica-ejecutado-por-la-fiscalia-general-de-la-republica.

42 «U-057-03-15», 27 de abril de 2015, www.jurisprudencia.gob.sv/DocumentosBoveda/DOC/1/2010-2019/2015/04/B817C.DOC.

43 «86-AP-M-2016», 25 de mayo de 2016, www.jurisprudencia.gob.sv/DocumentosBoveda/DOC/1/2010-2019/2016/05/C6D7B.DOC.

44 «U-057-03-15», 6.

45 Morgan Marquis-Boire et al., «Some Devices Wander by Mistake: Planet Blue Coat Redux», 9 de julio de 2013, https://citizenlab.ca/2013/07/planet-blue-coat-redux/.

2. Circles, Penlink, Conceptus, Hacking Team, NSO

El 6 de agosto de 2018 el periódico "Nuestro Diario" de Guatemala publicó un reportaje, basado en fuentes anónimas, que denuncia el uso de diversas herramientas de vigilancia en el país durante el gobierno de Otto Pérez Molina[46]. Si bien no hay documentos que sustenten su adquisición, las herramientas denunciadas existen y es importante que se investigue si ellas fueron efectivamente adquiridas y si vienen siendo utilizadas.

Entre las herramientas mencionadas en el artículo aparecen Circles, Penlink, Conceptus, HackingTeam, NSO y otros. Llama la atención el caso de HackingTeam, ya que en una investigación realizada por la organización Derechos Digitales, basada en correos y documentos filtrados por esta empresa, se menciona que la empresa negoció con el país. La Dirección de Análisis Criminal habría buscado capacitar a 200 agentes para que pudieran utilizar las herramientas ofrecidas por esta empresa. En este caso fue Ori Zoller quién lideró la negociación, aunque dentro de la información filtrada no existe evidencia de que se concretara la compra[47].

Por su parte, la investigación de Luis Sas en el medio "Nuestro Diario" menciona a empresas ligadas con Ori Zoller como las proveedoras de herramientas de vigilancia para la Dirección General de Inteligencia Civil (Digici). En el caso del software Galileo de HackingTeam señala que:

> Los documentos revelan negociaciones de Zoller con una empresa italiana para adquirir un software denominado Galileo a requerimiento de Manuel Antonio Alvarado Franco, exdirector de la Digici, a quien incluso le demostraron el alcance del producto espiando frente a él a una persona.[48]

Según el portal Guatecompras, en julio de 2017 la Dirección General de Inteligencia Civil del Ministerio de Gobernación quiso adquirir el software Penlink. El proceso se canceló aduciendo lo siguiente: "se finaliza anulado el presente concurso, debido a que se van a modificar y ampliar las especificaciones técnicas, derivado a lo complejo del Software solicitado."[49]

3. Magnet Axiom

En Guatemala, la Dirección General de Inteligencia Civil del Ministerio de Gobernación compró el software a la empresa ITD en julio de 2017. La contratación se hizo mediante adjudicación directa.[50]

3) Honduras

1. Hacking Team

Como ya se ha señalado, en 2015 esta empresa fue vulnerada de manera electrónica. Como consecuencia, sus correos electrónicos, así como archivos, se hicieron públicos. Según la investigación realizada por la organización Derechos Digitales en base a las filtraciones de Hacking Team, esta empresa fue contratado en Honduras [51].

Según esta investigación la Dirección Nacional de Investigación e Inteligencia (DNII) de Honduras habría gastado 355 000 euros en el año 2014. La compra la habría realizado a través de la empresa Nice representada en la región por Ori Zoller.

---

46 Sas, Luis Angel, «Espionaje ilegal del Gobierno: Aquí está la investigación de Nuestro Diario (Parte I)», Nómada, Guatemala., 7 de agosto de 2018, https://nomada.gt/pais/la-corrupcion-no-es-normal/espionaje-ilegal-del-gobierno-aqui-esta-la-investigacion-de-nuestro-diario-parte-i/.

47 Pérez de Acha, Gisela, «Hacking Team Malware para la Vigilancia en América Latina».

48 Sas, Luis Angel, «Espionaje ilegal del Gobierno: Aquí está la investigación de Nuestro Diario (Parte I)», Nómada, Guatemala., 7 de agosto de 2018, https://nomada.gt/pais/la-corrupcion-no-es-normal/espionaje-ilegal-del-gobierno-aqui-esta-la-investigacion-de-nuestro-diario-parte-i/.

49 «NOG: 6557961», Guatecompras - Sistema de Contrataciones y Adquisiciones del Estado de Guatemala, accedido 15 de enero de 2019, http://www.guatecompras.gob.gt/concursos/consultaDetalleCon.aspx?o=5&nog=6557961.

50 «Guatecompras - Detalle de un concurso», accedido 6 de febrero de 2019, http://www.guatecompras.gob.gt/concursos/consultaDetalleCon.aspx?o=5&nog=6557937.

51 Pérez de Acha, Gisela, «Hacking Team Malware para la Vigilancia en América Latina».

2. Verint

German Allan McNiel Rueda, subdirector nacional del Instituto Nacional Penitenciario (INP), fue parte de una delegación que representó al Instituto Nacional Penitenciario para la demostración de las instalaciones de los sistemas implementados por el cliente de Verint en los presidios de Trinidad y Tobago.[52] Fue delegado para ello por la Directora Nacional, Rosa Irene Gudiel Ardón, con el fin de atender la invitación hecha por Luis Fernando Suazo Barahona, Secretario Técnico del Gabinete de Defensa y Seguridad de la Presidencia de Honduras. Dicha actividad se realizó entre el 21 y el 24 de agosto de 2017.

En agosto de 2017, la empresa Verint Systems LTD solicitó solvencias de persona jurídica. Se trata de un trámite exigido cuando se quiere ofertar en el sistema público de compras. En aquel momento, su representante legal, según documentos oficiales del gobierno hondureño, era Claudia Lizeth Aguilera Granera.[53]

Por otro lado, Verint Systems LTD está reconocida como una empresa que se dedica al rubro de seguridad en el listado de proveedores del Estado de la Oficina Normativa de Contratación del Estado (ONCAE). Esto es así,desde el 13 de enero de 2016. Entonces figuraba como único socio un señor de nombre Pedro Eulalio Mejía.[54] Esto demuestra las intenciones de la empresa de ofertar para el Estado, no así que este haya adquirido el producto. En cualquier caso, el viaje de McNiel Rueda demuestra interés en el funcionamiento del mismo.

3. Cellebrite

En el informe sobre la situación de Derechos Humanos en Honduras para los años 2016 y 2017[55]realizado por el gobierno de este país, y financiado por la Unión Europea, se menciona explícitamente que el gobierno adquirió productos de Cellebrite entre otras herramientas:

> "Se adquirió equipo y software especializados como Cellebrite: Licencia que sirven para la extracción de datos (vaciado) de teléfonos; Avid Software: Herramienta tecnológica que sirve para la edición de video, conversión y codificador de extensiones forenses de video"

Además de Cellebrite, se menciona Avid Software que es un sistema forense para la edición de video. Por cuestiones de tiempo, no se pudo profundizar acerca de sus funcionalidades.

4) Nicaragua

1. Bluecoat

La ya mencionada investigación realizada por "Citizen Lab" en 2013 descubrió que entre los 83 países que ejecutaban los productos PacketShaper and ProxySG de BlueCoat se encontraba Nicaragua. En ese caso se encontraron 9 servidores con PacketShapper en Nicaragua.[56]

2. Verint

En Nicaragua, Verint es una marca registrada de la empresa estadounidense Verint Systems Inc. Así consta, en la solicitud al registro de Marca de Fábrica y Comercio de Nicaragua, realizada el 6 diciembre de 2011, misma que fue inscrita el 6 de noviembre de 2013. Dicho registro tiene una validez por 10 años.[57]

---

52 Gudiel Ardon, Rosa Irene, «Acuerdo de Delegación No. DN-INP-05-2017», 16 de agosto de 2017, https://portalunico.iaip.gob.hn/archivos/InstitutoNacionalPenitenciario/Regulaciones(normativa)/Acuerdos%20Institucional/2017/Acuerdo%20NO.%205.pdf.

53 «LISTADO DE SOLVENCIAS SOLICITADAS DE PERSONAS JURÍDICAS CORRESPONDIENTES AL MES DE AGOSTO - 2017», agosto de 2017, https://portalunico.iaip.gob.hn/archivos/(PGR)/Estructura/Registro%20Publico/2017/Solvencia%20Personas%20Juridicas%20Agosto%202017.pdf.

54 «Registro de Proveedores y Contratistas del Estado Enero 2016», enero de 2016, http://transparencia.scgg.gob.hn/descargas/temp_files/registros%20publicos%20oncae/Registro_Proveedores_y_Contratistas_enero_2016.pdf.

55 «Informe Derechos Humanos en Honduras 2016-2017» (Gobierno de la República de Honduras, diciembre de 2017), pag 10, http://www.rnp.hn/wp-content/uploads/2011/06/Informe_Derechos_Humanos_en_Honduras_2016-2017.pdf.

56 Morgan Marquis-Boire et al., «Some Devices Wander by Mistake: Planet Blue Coat Redux», 9 de julio de 2013, https://citizenlab.ca/2013/07/planet-blue-coat-redux/.

57 «La Gaceta Diario Oficial» (Gaceta Oficial de Nicaragua, 6 de noviembre de 2013), 12, http://www.pgr.gob.ni/PDF/2013/GACETAS/NOVIEMBRE/GACETA_211_06-11-2013.pdf.

Según la descripción realizada por el gestor al registro Mario Gutierrez Vasconcelos - Gestor (a) Oficioso (a) exponía que Verint Systems Inc. de Estados Unidos de América - solicitaba registro de Marca de Fábrica y Comercio: VERINT marca para, entre otras cosas: "aparatos para el registro, transmisión o reproducción de sonido o imágenes; soportes de registro magnéticos, discos acústicos específicamente, cintas pre-grabadas de vídeo, equipos (hardware) y programas (software) de casetes, dvds y cds. Computación en los campos de telecomunicaciones, seguridad y vigilancia digital, inteligencia de seguridad, redes de computadoras y de telecomunicación y multimedia, para monitorizar, adquirir, grabar."[58]

3. Encase

Los pliegos de un convenio de cooperación denominado "Proyecto Apoyo a Medidas de Prevención y de Control de Drogas y Crimen Organizado en Nicaragua", financiado por la Unión Europea y administrado por la Agencia Española de Cooperación Internacional para el Desarrollo (AECID) brindan información sobre la relación entre Nicaragua y Encase.[59] Se sabe que el gobierno de Nicaragua quiso comprar licencias para "EnCase: 1 Licencia por puesto de trabajo + PLSP por 3 años" y para "Licencias de IEF como complemento de Encase".

El documento además de productos de Encase, menciona herramientas como "Equipos de rastreo GPS para personas" o "Examinador de Correo", entre otros.

58 «La Gaceta Diario Oficial» (Gaceta Oficial de Nicaragua, 6 de diciembre de 2011), http://www.pgr.gob.ni/PDF/2013/GACETAS/NOVIEMBRE/GACETA_211_06-11-2013.pdf.

59 «PLIEGO DE CLÁUSULAS ADMINISTRATIVASPARTICULARES», 23 de marzo de 2017, 6, https://www.policia.gob.ni/wp-content/uploads/2017/03/PLIEGO-L.P.-06-2017-Compra-de-Equipamiento-Especializado-TICs.pdf.

Conclusiones

Se empezó este documento explicando las diversas formas en la que las comunicaciones pueden ser vigiladas. Según lo señalado, el monitoreo se puede hacer interceptando las comunicaciones de la red, lo cuál es posible con software como los provistos por Bluecoat, Verint o Penlink.

Luego se analizó la información que proveedores de servicios almacenan sobre sus usuarias/os. Empresas como Facebook, Google, Twitter y otras almacenan información sobre las personas que se conectan a sus plataformas. Los gobiernos, en casos de emergencia o a través de mecanismos legales, pueden solicitar información sobre las cuentas de las personas usuarias. Se vio que, salvo Nicaragua, todos los países han tenido la capacidad de solicitar información a estas empresas.

El *malware* es un software que se instala en teléfonos celulares o computadoras para tomar control y poder utilizarlos de forma remota. Se sabe, según las filtraciones de HackingTeam, que Honduras tendría este sistema en el 2015. Según estas mismas filtraciones, se veía que Guatemala se encontraba negociando. Por otro lado, a partir de la investigación realizada por Luis Sas, se podría sospechar que este país sí utilizó este sistema y que además habría adquirido el Pegasus de NSO.

El software forense es utilizado por los cuatro países, como también se utiliza en agencias policiales a nivel mundial. Marcas como Cellebrite, Encase o Axiom son utilizadas en estos países.

En la siguiente tabla se ve un resumen de las capacidades tecnológicas de cada país.

Tabla 3

Capacidades Conocidas por País					
País	**Red**	**Proveedor de Servicio**	**Internet / OSINT**	**Malware**	**Forense**
El Salvador	X	X	X		X
Guatemala	X	X	X	X	X
Honduras	X	X	X	X	X
Nicaragua	X		X		X

Fuente: elaboración propia

En este documento no se acusa sobre el mal uso de estas herramientas; sin embargo, se alerta sobre las capacidades de estas tecnologías cada vez más utilizadas por agencias estatales. La ciudadanía debe estar informada sobre las capacidades de este tipo de herramientas y sobre la forma en que las mismas podrían vulnerar derechos humanos y derechos constitucionales reconocidos en cada uno de los países vinculados a la privacidad[1].

La comunicación es un recurso estratégico que permite a la sociedad organizarse. Conocer las formas en las que esta puede ser vigilada permite tomar decisiones sobre cómo protegerlas. Estas medidas de protección deben venir desde el ámbito legal, pero también desde el tecnológico. Si bien el robo es ilegal, utilizamos cerraduras y candados porque las leyes no se cumplen siempre. De la misma manera, es importante utilizar cifrado y herramientas libres para proteger las comunicaciones.

1 El derecho a la privacidad deriva de lo expresado en el artículo 12 de la Declaración Universal de los Derechos Humanos: "Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques".