Privacidad y seguridad en internet: la web oscura (junio de 2016)

Boris A. Gómez
Universidad Tecnológica de Panamá
Artículo para "The Hacking Day - Project" – www.thehackingday.com

Resumen **- La privacidad y seguridad en las comunicaciones son inquietudes legítimas de quienes viven en regímenes represivos o, simplemente, de quienes desean evitar que sus actividades personales sean observadas. El enrutamiento de cebolla, como también se le conoce a la red Tor, fue diseñado especialmente para ofrecer esta clase de seguridad y privacidad, pero existen muchas dudas sobre su efectividad, por lo que en este artículo revisamos sus fortalezas y deficiencias. El artículo estuvo enfocado en Tor, por ser la tecnología de la web oscura más reconocida, respaldada y estudiada a nivel mundial, aunque es necesario anotar que la seguridad en internet no depende exclusivamente de Tor. La cadena de seguridad está compuesta de múltiples elementos que deben considerarse al momento de intentar resguardarnos en esta red, por lo que el desconocimiento de esta realidad puede ocasionar que la identidad y la ubicación de usuarios y sitios web ocultos sean reveladas.**

Abstract **- Privacy and security in communications are legitimate concerns of those living in repressive regimes or those who simply want to prevent their personal activities from being observed. The onion routing, as it is also known the Tor network, was designed especially to offer this security and privacy, but there are many doubts about its effectiveness, so in this article we reviewed its strengths and weaknesses. The article was focused on Tor, because this is the most recognized, supported and studied dark web technology worldwide, although it is necessary to note that the internet security does not depend exclusively on Tor. The safety chain is composed of multiple elements that must be considered when trying to protect ourselves in this network, so ignorance of this reality can cause the identity and location of users and hidden websites to be revealed.**

Palabras clave **- i2P, privacidad, Tor, web oscura (dark web, darknet), web profunda (deep web)**

I. Introducción

Activistas, disidentes políticos, periodistas en países en conflicto o en regímenes represivos, defensores de los derechos humanos, agentes encubiertos y todo aquel que desea evitar que sus actividades sean vigiladas, en ocasiones necesitan comunicarse, navegar en internet o compartir información de forma libre, confidencial y segura. Las dudas naturales que suelen surgir son:

- ¿qué hacer para ocultar identidad y ubicación?
- ¿cómo garantizar la privacidad de sus comunicaciones (telefónicas, mensajes instantáneos, foros o correo electrónico)?
- ¿cómo compartir archivos de manera confidencial?
- ¿cómo conservar información en sus dispositivos, sin que otras personas tengan acceso al contenido, aunque obtengan acceso a los dispositivos?

Existen diversas tecnologías para resguardar privacidad y seguridad, y la web oscura es una de las más reconocidas, sin embargo, esa seguridad que brinda conduce a que muchos delincuentes oculten sus actividades en ella. Las tecnologías que mejor representan a la web oscura son Tor e i2P, siendo Tor la red más utilizada y estudiada a nivel mundial, por lo que ha estado expuesta a múltiples ataques.

Por otra parte, la web oscura es un reto para las autoridades quienes, además de identificar, recopilar evidencias y ubicar a los delincuentes que se ocultan en ella, necesitan probar, en los tribunales, que esas evidencias han sido recopiladas conforme a la ley.

Es necesario anotar, finalmente, que para desarrollar este artículo se compiló información de diversas fuentes en internet, a fin de conocer mejor el nivel de privacidad y seguridad que se obtiene de la web oscura.

II. Privacidad y Seguridad

Para resguardar privacidad y seguridad existen diferentes tecnologías. Al respecto, la empresa de seguridad informática Cyberkov publicó una lista de productos y servicios recomendados (el documento original está escrito en árabe) [1]:

- Red social para el envío de mensajes: Twitter.
- Falsear la información que se almacena con las fotografías digitales (geo-localización), antes de publicar las fotos (útil para corresponsales): Mappr.
- Dispositivos móviles con características avanzadas para cifrar texto, voz y vídeo: Blackphone y Cryptophone.
- Alternativas cuando se han cortado las comunicaciones: Twitter vía SMS, redes wifi privadas, radios de comunicación de corto alcance (walkie talkies, tomando en consideración que la comunicación no es cifrada), aplicaciones que no requieren de redes de comunicación como: FireChat, Tin Can y The Serval Project.
- Redes privadas virtuales (VPN): Freedome y Avast SecureLine.
- Navegación en internet: Tor, Orweb, Onion Browser, Aviator (Google denunció la existencia de múltiples agujeros de seguridad en Aviator), Yandex OperaMini.
- Cifrado de archivos y dispositivos, en caso de pérdida o confiscación de equipos: TrueCrypt (descontinuado), VeraCrypt, BitLocker y Crypto SSD.
- Correo electrónico: Hushmail, ProtonMail, Tutanota, que

permiten cifrar los mensajes y archivos adjuntos.

- Mensajería instantánea: Threema, Telegram, SureSpot, Wickr, Cryptocat, IO SwissCom, PQChat, Sicher e iMessage.
- VoIP cifrado: Linphone, IO Swisscom, RedPhone y Signal; productos y servicios de la empresa Silent Circle y el servicio FaceTime.
- Almacenamiento en la nube: MEGA, SpiderOak, SugarSync, Copy.com.

A. *Privacidad y seguridad en la web oscura*

Antes de definir web oscura, es necesario diferenciarla de la web profunda.

Se denomina web profunda a todo lo que está en la web que no es indexado por buscadores como Google o Yahoo, por ejemplo, las intranets, las bases de datos de empresas y los sitios web accesibles solo bajo subscripción. Se estima que un 96% de todos los datos en internet son invisibles a estos buscadores.

La web oscura, por el contrario, es una fracción de la web profunda, diseñada específicamente para ocultar la identidad y resguardar la seguridad de los usuarios y de los sitios web que aloja. Se respalda en la tecnología del cifrado de datos y, por lo general, utiliza redes, protocolos y puertos con tecnología no estándar, por lo que solo puede ser accedida a través de software especializado.

Es importante anotar que las fallas en la anonimidad de la web oscura dependen de múltiples factores, por ejemplo:

- El sistema operativo utilizado.
- Las fallas de seguridad (*bugs*) en el sistema operativo y en las aplicaciones o librerías que intervienen en el proceso.
- Los errores humanos:
  - Ingreso a sitios que registran datos o actividades de los usuarios.
  - Abrir documentos descargados de la web oscura mientras se está en línea.
  - Instalar o habilitar extensiones no seguras en el navegador de internet.
  - Sistema operativo y aplicaciones desactualizadas.
  - Configuraciones personalizadas de las aplicaciones, de forma tal que diferencie a un usuario del resto de los usuarios en la red.

B. *Tecnología de la web oscura*

Algunas de las tecnologías existentes para proporcionar anonimidad en internet son:

- Dominios de Nivel Superior alternativos (*rogue Top Level Domains*): permiten la comunicación en internet sin necesidad de utilizar los dominios de la ICANN.
- Freenet: permite navegar en internet de forma anónima, compartir archivos, chatear, comunicarse en foros y alojar sitios web que solo pueden ser accedidos a través de Freenet.
- PrivaTegrity: es un proyecto que se propone como alternativa a Tor pero que, según su creador, permitirá atacar el cibercrimen a través de una puerta trasera o *backdoor*.
- Astoria: es un proyecto descontinuado de software cliente para conectarse a la red Tor, según sus desarrolladores, capaz de garantizar que el tráfico no pase por enrutadores controlados por organizaciones o piratas informáticos. Los autores de este proyecto revelaron datos sobre las actividades en la web oscura.
- i2P y Tor: son descritos a continuación.

1) i2P

Es una red anónima que compite con Tor. Aunque no está especialmente diseñada para ocultar que un usuario está utilizando esta red, sí lo está para ocultar los sitios web a los que el usuario ingresa y las actividades que realiza.

Garantiza un alto nivel de anonimidad. Es un software abierto y gratuito, útil para correo electrónico, chats, blogs, grupos de noticias y compartición de archivos. Utiliza el dominio .i2p y conmutación de paquetes (mientras que Tor utiliza conmutación de circuitos).

a) ¿Cómo funciona i2P?

Para enviar datos, i2P establece dos rutas unidireccionales, una para enviar y otra para recibir tráfico, con varias capas de cifrado de los datos y, al igual que Tor, cada nodo en la ruta solo puede descifrar una capa pero, por su característica de utilizar dos túneles, quien pretenda realizar análisis de tráfico requiere del doble de nodos que Tor.

En principio, todos los usuarios en esta red pueden actuar como enrutadores de los otros usuarios, por lo que no hay nodos de entrada y de salida oficialmente establecidos, como ocurre con Tor.

b) Algunas ventajas de i2P sobre Tor [2]

- Las APIs de i2P están diseñadas específicamente para anonimidad y seguridad.
- Es distribuido y auto-organizado.
- Los servidores de directorios (floodfill) no son fijos (al no existir un directorio de nodos de entrada/salida, es más difícil bloquear el acceso a esta red).
- Los pares son seleccionados continuamente según su rendimiento y categoría.
- Resistente a fallos debido a que usa varios túneles en paralelo.
- Los túneles de i2P tienen una vida corta, reduciendo el número de muestras que un atacante puede usar para lograr un ataque activo.

c) Ataques a los que puede exponerse la red i2P [3]

- Ataque de fuerza bruta: monitorizando todos los mensajes que pasan por los nodos, un atacante podría determinar las rutas que siguen los mensajes.
- Ataque de sincronización: al monitorizar el tráfico y relacionar los tiempos de respuesta de las aplicaciones (existen patrones reconocibles en la frecuencia de los mensajes), un atacante puede descartar enlaces y determinar las rutas utilizadas por sus víctimas.
- Ataque por intersección: estableciendo contacto frecuente

con una víctima, un atacante podría conocer los usuarios activos en la red.

- Ataques de denegación de servicio: un atacante podría consumir más recursos de los que aporta a la red, crear un gran número de pares en la red que no proporcionen recursos o que denieguen nuevas conexiones, inundar la red con mensajes, sobrecargar el CPU de pares al solicitarles que ejecuten operaciones consumidoras de recursos, afectar la red al convertirse en uno de los servidores de directorio (*floodfill*).
- Ataque de etiquetado: un atacante ubicado en la puerta del túnel de entrada y más adelante en el mismo túnel, podría determinar que está en el mismo túnel y conspirar para realizar acciones maliciosas.
- Ataque de partición: un adversario poderoso podría fragmentar la red al desconectar los enlaces de las víctimas.
- Ataque de cosechado: un atacante, funcionando como enrutador, podría obtener un listado de los usuarios que utilizan i2P.
- Identificación mediante análisis de tráfico: monitorizando el tráfico de entrada y de salida de un enrutador, un atacante podría identificar que un usuario específico está utilizando i2P.
- Ataque Sybil: un atacante podría crear un gran número de nodos fraudulentos para montar otros tipos de ataques.
- Ataque por agotamiento de par: un atacante, funcionando como enrutador, podría forzar a que el túnel se forme sólo con enrutadores fraudulentos.

2) Tor

La red Tor tiene su origen en el Laboratorio de Investigación Naval de los Estados Unidos y fue diseñada con el objetivo de proteger las comunicaciones navales, de forma tal que enemigos no pudieran rastrear sus mensajes ni detectar la posición de sus buques. Actualmente es una red abierta y gratuita. Es utilizada para prevenir que intrusos en internet identifiquen, conozcan la ubicación física o los hábitos de navegación de los usuarios, además de ocultar la identidad y la localización los sitios web que aloja. Utiliza el dominio .onion.

Es respaldada por organismos de derechos humanos y ha sido financiada por el Departamento de Estado y el Departamento de Defensa de los Estados Unidos [4].

La decisión del gobierno estadounidense de apoyar el desarrollo de una herramienta de privacidad y seguridad robusta y segura (como Tor) nos indica que reconoce que sus beneficios son superiores a los posibles aspectos negativos de la misma.

En marzo de 2011 Tor recibió, de la Free Software Foundation, el premio para proyectos de beneficio social, por "haber permitido que, aproximadamente, 36 millones de personas de todo el mundo, usando software libre, hayan experimentado libertad de acceso y de expresión en Internet manteniendo su privacidad y anonimato. Su red ha resultado crucial en los movimientos disidentes de Irán y Egipto" [5].

Está constituida por una red mundial de voluntarios (2052 nodos de entrada, 7128 enrutadores y 912 nodos de salida) [6]. Es accedida por aproximadamente 2.5 millones de usuarios diarios [7].

a) ¿Cómo funciona Tor?

A esta red se accede con el navegador Tor (denominado *onion proxy* o OP) que debe estar instalado en la computadora cliente. El OP establece una ruta compuesta por tres nodos de retransmisión (*onion routers* o OR) y tres llaves de cifrado independientes, una para cada uno de los nodos de retransmisión, con las cuales se cifra el dato tres veces, iniciando con la llave del último nodo. A continuación, el dato es enviado al primer nodo (*guard node*) del circuito. Éste elimina la primera capa de cifrado y retransmite el dato al siguiente nodo. El proceso se repite hasta alcanzar el nodo de salida (*exit node*), que elimina la última capa de cifrado y envía el dato al destino (ver ejemplo en la figura 1 a continuación).

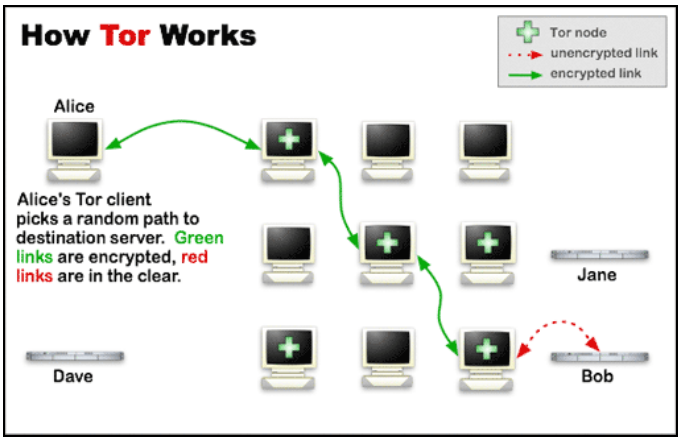

Fig. 1. How Tor Works. Fuente: The Tor Project

b) Características de Tor

- Sólo el cliente Tor conoce las tres llaves de cifrado.
- Cada nodo en el circuito conoce solamente el nodo previo y el siguiente.
- El nodo de salida envía el dato al destino sin cifrar, excepto que el destino maneje su propio protocolo de cifrado.
- La computadora de destino no conoce la identidad ni la ubicación del cliente.

c) Algunas Ventajas de Tor sobre i2P [2]

- Posee una base de usuarios muchos más grande, más desarrolladores con experiencia, más fondos y está mejor estudiado y documentado.
- Su control centralizado reduce la complejidad para cada nodo y permite un mejor control de los nodos malignos que intenten formar parte de la red.
- Ha resuelto algunos problemas de escala que aún deben ser abordados en i2P.
- Es la mejor opción para usuarios que solo necesitan acceder, de forma anónima, a la web visible [8].

III. Criminalidad en la web oscura

Al ingresar a la web oscura se puede observar que en ella existen actividades ilegales. Daniel Moore y Thomas Rid señalaron, en su artículo "Cryptopolitik and the Darknet", que el uso más común de Tor es para ocultar servicios como la venta de drogas, las finanzas ilícitas y la pornografía con violencia, niños y animales [9].

En base a los resultados del proyecto Artemis, investigadores han señalado que la mayoría de los sitios web ocultos comercian drogas, armas, códigos maliciosos, servicios de *hacking*, códigos para explotación de vulnerabilidades, denegación de servicio, números de tarjetas de crédito y pornografía infantil, además de contener una gran cantidad de documentos sobre actividades políticas [10].

A continuación, algunas actividades criminales desarticuladas.

A. Mercado negro de tarjetas de crédito

- Dark Market: sitio web dedicado a la venta de información de tarjetas de crédito, contraseñas robadas y equipos para realizar fraude electrónico. Fue infiltrado por un agente encubierto de la Oficina Federal de Investigaciones (FBI) y clausurado en el año 2008, en una operación encubierta que duró dos años [11], [12].
- Darkode: sitio web dedicado a la venta de servicios de *hacking* e información de tarjetas de crédito, *botnets*, correo basura (*spam*) y otros. Fue creado en el año 2007, infiltrado en una operación internacional coordinada por el FBI y cerrado en julio de 2015. Fue denominado, por Europol, como el foro de cibercriminales angloparlantes más prolífico hasta la fecha. Sin embargo, dos semanas después de clausurado reapareció en internet con mayores controles de seguridad y operando en la red Tor [13], [14].

B. Lavado de dinero

- Liberty Reserve: sitio web dedicado al negocio financiero ilegal. Fue cerrado por las autoridades en mayo de 2013, en lo que se llamó el mayor caso de lavado de dinero del mundo [15].

C. Pornografía y abuso infantil

- PedoBook: sitio web dedicado a la pornografía infantil. Se ocultaba en Tor. Su administrador, Aaron McGrath, fue arrestado en noviembre de 2012, pero las autoridades mantuvieron el servicio en funcionamiento en sus propios servidores, con el fin de descubrir la identidad de sus visitantes. El sitio web fue cerrado en diciembre de ese mismo año.

  Timothy DeFoggi, director de ciberseguridad de Health and Human Services (HHS) de los Estados Unidos, fue acusado de tráfico de pornografía infantil, explotación sexual de niños, intento de violación y asesinato violento de niños, luego que las autoridades infiltraran PedoBook. Fue encontrado culpable en agosto del año 2014 y sentenciado a 25 años de prisión [16].
- Freedom Hosting: era conocido como el más grande servicio de alojamiento en la web profunda. Utilizaba Tor e incluía pornografía infantil. Fue creado en el año 2008 (por Eric Eoin Marques, señalado como el más grande distribuidor de pornografía infantil) y cerrado en agosto de 2013 en base a la denominada Operation Darknet, dirigida contra los sitios web de pornografía infantil. La operación fue realizada por la asociación de activistas Anonymous [17], [18].
- PlayPen: era considerado como el sitio web de pornografía infantil más grande en internet en ese momento. Se ocultaba en la red Tor. Además de contenido con prácticas sexuales y abuso a menores, contenía instrucciones para evitar ser detectados por las autoridades. Fue creado en agosto de 2014 y cerrado por el FBI en febrero de 2015. El FBI mantuvo el sitio abierto en sus propios servidores hasta el 4 de marzo de ese año, con lo que logró identificar a 1,300 visitantes [19].

D. Estafa

- Sheep Marketplace: era un mercado negro oculto en la web oscura. Cesó operaciones de forma fraudulenta en diciembre de 2013. Fue considerado el cierre fraudulento más grande conocido de la web oscura. Operaba en Tor [20], [21].
- Evolution: era considerado el más grande mercado negro de drogas en internet. Inició operaciones en enero de 2014 y cerró en marzo de 2015, en un aparente cierre fraudulento realizado por sus administradores, quienes se retiraron con 12 millones de dólares en *bitcoins* de sus clientes. Operaba en Tor [22], [23], [24].

E. Tráfico de drogas

- Agora: se dedicaba a vender productos legales e ilegales. Inició operaciones en el año 2013. Luego del cierre de Evolution, y por el alto nivel de confianza que brindaba a sus clientes, se convirtió en el más grande mercado negro de drogas en la web oscura. Operaba en la red Tor y todas las transacciones se realizaban utilizando *bitcoins*. A finales del año 2015 los administradores del sitio anunciaron el cierre del mismo [25], [26].

F. Artículos científicos gratuitos

- La estudiante Alexandra Elbakyan, de Kazakhstan, creó en el año 2011 el sitio web Sci-Hub, que permitía descargar artículos científicos de internet sin necesidad de suscripción ni pago, utilizando una herramienta que utilizaba cuentas pertenecientes a subscriptores válidos. El sitio fue cerrado a finales del año 2015, pero reapareció en la red Tor. Actualmente se encuentra en un pleito legal, sin embargo, investigadores, artistas y escritores se han unido en protesta por las acciones legales en su contra [27], [28].

G. Servicios múltiples

- Atlantis: mercado negro en línea dedicado a la venta de drogas, servicios de *hacking* y otros. Fue creado en el año 2013 y clausurado ese mismo año por los propios administradores, según dicen, por razones de seguridad. Utilizaba la red Tor y los pagos se realizaban con *bitcoins* y *litecoins* [29], [30], [31].
- SilkRoad: sitio web dedicado al lavado de dinero, *hacking*, tráfico de drogas, venta de pasaportes falsos y sicariato. Fue creado en el año 2011 y cerrado en el año 2013. Para ocultar sus actividades, utilizaba Tor y *bitcoins*. El FBI señala que pudo identificar a su administrador sin necesidad de romper la seguridad de Tor [32], [33].
- SilkRoad 2.0: sitio web dedicado a la venta de armas, droga e información privada. Fue creado en noviembre de 2013 y cerrado en noviembre de 2014 en una acción internacional de la policía europea (Europol), del órgano judicial de la Unión Europea (Eurojust), del FBI y del Servicio de Inmigración y Control de Aduanas de los Estados Unidos (ICE Homeland Security Investigations), en una operación dirigida a cerrar los mercados negros que operaban en la red Tor.

  Además de SilkRoad 2.0 fueron cerrados sitios web como: Cloud 9 e Hydra, dedicados a la venta de drogas; Pandora, Blue Sky, Topix, Flugsvamp, Cannabis Road y Black Market, dedicados al contrabando; Cash Machine, Cash Flow, Golden Nugget y Fast Cash, dedicados al lavado de dinero.

  En enero de 2015, SilkRoad 2.0 reapareció con el nombre "Silk Road Reloaded". En esta ocasión en la red i2P y con soporte a múltiples monedas electrónicas (*bitcoin*, *anoncoin*, *darkcoin*, *dogecoin*, *altcoin*) [34], [35], [36], [37].
- TheRealDeal Market: sitio web basado en Tor y *bitcoins*, dedicado al lavado de dinero, servicios de *hacking*, software para la explotación de vulnerabilidades, cuentas robadas y drogas. Inició operaciones en el año 2015 y cerró temporalmente en julio de ese mismo año. Reapareció unos días después, luego que uno de sus administradores fuera liberado por las autoridades. El arresto y liberación de uno de sus administradores sembró dudas entre los usuarios del sitio [38], [39], [40].

IV. Investigaciones sobre Tor

Como se mencionó con anterioridad, son múltiples los factores que intervienen para garantizar privacidad y seguridad en internet y que pueden constituirse en el punto de falla de la cadena de seguridad.

En lo referente, específicamente, a la seguridad de Tor, a continuación algunos estudios del mismo:

- En el año 2004, Roger Dingledine, Nick Mathewson y Paul Syverson, en su artículo "Tor: the second-generation onion router", señalaron diferentes tipos de ataques a los que podría estar expuesta la red Tor, entre ellos: la monitorización de los patrones de tráfico en la red; el acceso a los contenidos que no están cifrados entre el nodo de salida y el sitio web de destino; la identificación de los usuarios con configuraciones personalizadas (que los hacen diferentes del resto de los usuarios); la monitorización y correlación de tiempos del tráfico en ambos extremos del circuito [41].
- En septiembre de 2007, Dan Egerstad, experto en seguridad informática, señaló que había creado nodos de salida en la red Tor y que al monitorizar y controlar toda la información que salía por estos nodos, logró conseguir contraseñas de cuentas de correo de embajadas, empresas y organizaciones de derechos humanos. Fue arrestado en noviembre de ese mismo año [42].
- En el año 2008, investigadores de la Universidad de Colorado y de la Universidad de Washington, publicaron un estudio en el que indicaban que controlando un nodo de salida, podrían identificar el tipo de tráfico que cruzaba la red Tor y los sitios web a los que accedían los usuarios. Además, controlando un nodo de entrada podrían identificar las direcciones IP de numerosos usuarios de Tor [43], [44].
- En la conferencia DEFCON del año 2008, se presentó el tema "Deanonymizing Tor", en donde se planteó que debido a las características del diseño de Tor, todos los nodos que participaran en un circuito de esta red podrían ser identificados [45].
- En el año 2013, investigadores de la Universidad de Luxemburgo, en su artículo "Trawling for Tor Hidden Services: Detection, Measurement, Deanonymization", señalaron fallas tanto en el diseño como en la implementación de Tor. Indicaron que con pocos recursos y apropiándose de uno o más nodos de entrada era posible identificar sitios ocultos y medir la cantidad de accesos al mismo, con lo cual un atacante podría priorizar sus ataques [46].
- En el artículo "RAPTOR: Routing Attacks on Privacy in Tor", en el año 2015, investigadores señalaron que un atacante controlando un nodo de entrada y de salida de la red Tor podría identificar a los usuarios de Tor con hasta 95% de precisión, mediante la suite para ataques denominada RAPTOR [47].
- En el año 2015, investigadores del Massachusetts Institute of Technology (MIT), del Qatar Computing Research Institute (QCRI) y de Qatar University indicaron que los usuarios de Tor y los sitios web ocultos podrían ser identificados con un alto grado de certeza, mediante monitoreo pasivo [48].

V. Vigilancia de la web oscura

La abundante actividad criminal en la web oscura ha provocado repudio de la comunidad y de las autoridades, por ello algunos gobiernos invierten grandes sumas de dinero en tecnología para monitorizar las actividades que se ocultan en ella. Tal es el caso de agencias como el FBI y la NSA de los Estados Unidos y el Centro de Seguridad e Inteligencia del Reino Unido (Government Communications Headquarters - GCHQ). Por otra parte, se conoce que Rusia ofrece

recompensa para quien logre romper la seguridad de la red Tor [49] y países como Irán, Arabia Saudita, Turquía, Grecia, China, Rusia, India, Indonesia y Sudan bloquean el acceso a esta red [50].

Con relación al FBI, sus intereses manifiestos son los temas de seguridad nacional (como el terrorismo), los asesinatos en serie, el espionaje, el crimen organizado, el cibercrimen, la pedofilia y otros [51].

Mientras que la NSA es responsable de recolectar, analizar y proporcionar señales de inteligencia extranjera a autoridades y fuerzas militares [52]. Cuenta con una unidad especializada de hackers, denominada Tailored Access Operations (TAO), cuyo objetivo es el desarrollo de productos para vulnerar la red, infiltrar computadoras y recopilar información de los usuarios, en busca de amenazas a la seguridad nacional [53].

Similarmente, el GCHQ tiene el propósito defender los sistemas del gobierno contra amenazas cibernéticas, proporcionar apoyo a las fuerzas armadas y mantener la seguridad pública [54].

En consecuencia, si la conclusión es que la web oscura puede ser vulnerada y, además, existen organismos que realizan vigilancia masiva de las comunicaciones a nivel mundial ¿cómo es posible que persistan actividades ilegales en ella?

La respuesta a esta interrogante podría estar en el hecho de que el objetivo primordial del enrutamiento de cebolla ha sido, desde su creación, el encubrimiento de las operaciones militares y de inteligencia de los organismos de seguridad de los Estados Unidos. No obstante, si este fuera utilizado exclusivamente por los departamentos de seguridad nacional, quien lo utilice estaría revelando que pertenece a uno de esos departamentos. Como consecuencia, surgió la necesidad de abrir esta red (Tor) al público en general (cuanto mayor sea el número de usuarios en esta red y mayor la diversidad de actividades, mejor será el encubrimiento) [55].

Otros posibles elementos a considerar son:

- Las autoridades (FBI, NSA, etc.) podrían estar al acecho, preferentemente, de grandes organizaciones criminales.
- Los sitios web ocultos son cerrados cuando sus administradores perciben alguna amenaza y son reabiertos con nuevas y mejores medidas de seguridad.
- El desarrollo de investigaciones y soluciones a las vulnerabilidades de la web oscura brinda confianza en la fortaleza del sistema.
- Las complejidades legales asociadas con la intrusión en las computadoras y con la vigilancia masiva de las actividades en la red, son factores a tomar en cuenta por las autoridades al momento de realizar acciones en contra de actividades delictivas, de forma tal que puedan sustentar, ante los tribunales, los procedimientos realizados.

Es necesario anotar que solo el 5% de los operadores del mercado negro, asociados con Tor-Bitcoin, han sido desmantelados [56].

A. *Aspectos Legales de la vigilancia de la red*

Las autoridades reconocen la importancia de herramientas como Tor, puesto que ellas mismas las utilizan para vigilancia, actividades de inteligencia e infiltración de computadoras. Un ejemplo son las unidades de policía de Holanda y Bélgica, quienes han sido capacitadas en el uso de Tor [57].

El dilema con la vigilancia masiva de las comunicaciones, en busca de actividades criminales, es al acceso a información no relacionada con los delitos investigados.

B. *Memex*

En la lucha contra las actividades ilegales en internet (en especial, el tráfico de seres humanos), la Agencia de Proyectos de Investigación Avanzada de Defensa de Estados Unidos (DARPA) está desarrollando un rastreador de páginas web al que ha denominado Memex. Su objetivo es indexar y organizar el contenido de millones de páginas de la web profunda, con base en la relación existente entre las páginas, a partir de un tema particular, lo que puede ser aprovechado por militares, gobierno y empresas. La agencia expresa que el propósito de Memex no es vulnerar el anonimato de la red ni acceder a información privada.

VI. Conclusión

Actualmente Tor es el servicio de privacidad y seguridad en internet mejor reconocido a nivel internacional, con una comunidad que le brinda soporte y millones de usuarios diarios, sin embargo, su anonimidad no es absoluta, por lo que si su seguridad e integridad personal dependen del anonimato en la red, es recomendable que limite la cantidad de veces que ingresa y el tiempo que permanece dentro de la misma, a fin de minimizar la efectividad de los análisis de su actividad en la red, sin olvidar que mientras más nodos y usuarios formen parte de esta red, mayor será la seguridad obtenida.

Hay que ser conscientes que esta tecnología aún está en desarrollo y que, igual que hay desarrolladores a favor del secreto en la red, también hay quienes tratan de quebrantarla.

Por otro lado, los que realizan investigaciones en la web oscura deben ser conscientes que el concepto de ilegalidad depende de cada país pero que, en general, ingresar a sitios web en donde se mercadean drogas, armas y similares no es ilegal (lo ilegal es comprar drogas con intensión de distribuirla, por ejemplo), en cambio, sí es ilegal ingresar y acceder a materiales relacionados con la pedofilia y el abuso infantil.

Finalmente, si usted accede a contenidos que tengan relación con el terrorismo o similares, se expone a que sus actividades sean rastreadas de ese momento en adelante.

Referencias

[1] A. AlAli. “Los derechos en la Franja de Gaza!!”, *blog.cyberkov.com*, 26-julio-2014. [en línea]. Disponible en: https://blog.cyberkov.com/1814.html.

[2] “Comparación de i2p con Tor”, *geti2p.net*. [en línea]. Disponible en: https://geti2p.net/es/comparison/tor. [Consulta: 31 marzo 2016].

[3] “i2P's Threat Model”, *geti2p.net*. [en línea]. Disponible en: https://geti2p.net/en/docs/how/threat-model.

[Consulta: 31 marzo 2016].

[4] "Consolidated Financial Statements and Reports Required for Audits in Accordance with Government Auditing Standards and Omb Circular A-133", *geti2p.net*. [en línea]. Disponible en: https://www.torproject.org/about/findoc/2012-TorProject-FinancialStatements.pdf.

[5] J. Sullivan. "2010 Free Software Awards announced", *Free Software Foundation*, 22-3-2011. [en línea]. Disponible en: http://www.fsf.org/news/2010-free-software-awards-announced.

[6] "Tor Network Status". [en línea]. Disponible en: https://torstatus.blutmagie.de. [consulta: 30 marzo 2016].

[7] L. Kelion. "Tor Project's struggle to keep the 'dark net' in the shadows", *BBC News*, 22-8-2014. [en línea]. Disponible en: http://www.bbc.com/news/technology-28886465.

[8] F. Astolfi, J. Kroese y J. Oorschot. "I2P - The Invisible Internet Project". [en línea]. Disponible en: http://mediatechnology.leiden.edu/images/uploads/docs/wt2015_i2p.pdf.

[9] D. Moore y T. Rid, *Cryptopolitik and the Darknet*, 1a ed., vol. 58, pp. 7-38. [en línea]. Disponible en: https://www.iiss.org/en/publications/survival/sections/2016-5e13/survival--global-politics-and-strategy-february-march-2016-44d5/58-1-02-moore-and-rid-9204.

[10] P. Paganini y R. Amores. "Project Artemis - OSINT activities on Deep Web", *Infosec Institute*, 1-7-2013. [en línea]. Disponible en: http://resources.infosecinstitute.com/project-artemis-osint-activities-on-deep-web.

[11] C. Davies. "Welcome to DarkMarket – global one-stop shop for cybercrime and banking fraud", *theguardian*, 14-1-2010. [en línea]. Disponible en: http://www.theguardian.com/technology/2010/jan/14/darkmarket-online-fraud-trial-wembley.

[12] DarkMarket. [en línea]. Disponible en: https://en.wikipedia.org/wiki/DarkMarket.

[13] "Cybercriminal Darkode Forum Taken Down Through Global Action", *Europol*, 15-7-2015. [en línea]. Disponible en: https://www.europol.europa.eu/content/cybercriminal-darkode-forum-taken-down-through-global-action.

[14] Dark0de. [en línea]. Disponible en: https://en.wikipedia.org/wiki/Dark0de.

[15] "Founder of Liberty Reserve Pleads Guilty to Laundering More Than $250 Million through His Digital Currency Business", *U.S. Department of Justice*, 29-1-2016. [en línea]. Disponible en: https://www.justice.gov/opa/pr/founder-liberty-reserve-pleads-guilty-laundering-more-250-million-through-his-digital.

[16] "HHS Security Director Sentenced to 25 Years for Tor-Network-Based CP", *DeepDotWeb*, 6-1-2015. [en línea]. Disponible en: https://www.deepdotweb.com/2015/01/06/sentenced-to-25-tor-network-cp.

[17] V. Buterin. "Freedom Hosting Taken Down, Founder Arrested, Users fed Javascript Exploits", *Bitcoin Magazine*, 5-8-2013. [en línea]. Disponible en: https://bitcoinmagazine.com/articles/freedom-hosting-taken-down-founder-arrestes-users-fed-javascript-exploits-1375664047.

[18] Freedom Hosting. [en línea]. Disponible en: https://en.wikipedia.org/wiki/Freedom_Hosting.

[19] "FBI Ultimate Hack Job, 1300 Computers Take Down", *DeepDotWeb*, 8-1-2016. [en línea]. Disponible en: https://www.deepdotweb.com/2016/01/08/fbi-ultimate-hack-job-1300-computers-take-down.

[20] "Dark marketplace closes after theft of £3m in bitcoins", *BBC News*, 2-12-1013. [en línea]. Disponible en: http://www.bbc.com/news/technology-25185225.

[21] "Breaking: Sheep Marketplace Owner Arrested", *DeepDotWeb*, 27-3-2015. [en línea]. Disponible en: https://www.deepdotweb.com/2015/03/27/breaking-sheep-marketplace-owner-arrested.

[22] "Dark Web's 'Evolution Market' Vanishes", *Krebs on Security*, 18-3-2015. [en línea]. Disponible en: https://krebsonsecurity.com/2015/03/dark-webs-evolution-market-vanishes.

[23] N. Woolf. "Bitcoin 'exit scam': deep-web market operators disappear with $12m", *theguardian*, 18-3-2015. [en línea]. Disponible en: http://www.theguardian.com/technology/2015/mar/18/bitcoin-deep-web-evolution-exit-scam-12-million-dollars.

[24] Evolution (marketplace). [en línea]. Disponible en: https://en.wikipedia.org/wiki/Evolution_(marketplace).

[25] R. Price. "One of the largest dark web drug marketplaces is closing down in a surprisingly professional manner", *Business Insider*, 26-8-2015. [en línea]. Disponible en: http://uk.businessinsider.com/dark-web-drug-market-agora-closing-down-temporarily-2015-8.

[26] Agora (online marketplace). [en línea]. Disponible en: https://en.wikipedia.org/wiki/Agora (online_marketplace).

[27] K. Waddell. "The Research Pirates of the Dark Web", *The Atlantic*, 9-2-2016. [en línea]. Disponible en: http://www.theatlantic.com/technology/archive/2016/02/the-research-pirates-of-the-dark-web/461829/?utm_source=SFFB.

[28] Alexandra Elbakyan. [en línea]. Disponible en: https://es.wikipedia.org/wiki/Alexandra_Elbakyan.

[29] A. Berry. "Atlantis, Illegal Online Drug Marketplace, Forced To Shut Down 'Due To Security Reasons Outside Of Our Control'", *International Business Times*, 21-9-2013. [en línea]. Disponible en: http://www.ibtimes.com/atlantis-illegal-online-drug-marketplace-forced-shut-down-due-security-reasons-outside-our-control.

[30] D. Gayle. "Inside Atlantis: The online black market that lets users buy and sell drugs, forgeries and hacking services anonymously", *MailOnline*, 28-6-2013. [en

línea]. Disponible en: http://www.dailymail.co.uk/sciencetech/article-2350952/Inside-Atlantis-The-online-black-market-lets-users-buy-sell-drugs-forgeries-hacking-services-anonymously.html.

[31] Atlantis (market). [en línea]. Disponible en: https://en.wikipedia.org/wiki/Atlantis_(market).

[32] D. Leinwand. “How FBI brought down cyber-underworld site Silk Road”, *USA Today*, 15-5-2014. [en línea]. Disponible en: http://www.usatoday.com/story/news/nation/2013/10/21/fbi-cracks-silk-road/2984921.

[33] S. Kerner. "Snowden Leaks Show NSA Targets Tor", eWeek, 4-10-2013. [en línea]. Disponible en: http://www.eweek.com/security/snowden-leaks-show-nsa-targets-tor.html.

[34] J. Cox. “Silk Road 2.0 Was Just Shut Down by the FBI”, *Motherboard*, 6-11-2014. [en línea]. Disponible en: http://motherboard.vice.com/read/silk-road-2-has-been-seized-by-the-fbi.

[35] A. Greenberg. “Global Web Crackdown Arrests 17, Seizes Hundreds of Dark Net Domains”, *Wired*, 11-7-2014. [en línea]. Disponible en: http://www.wired.com/2014/11/operation-onymous-dark-web-arrests.

[36] J. Cox. “'Silk Road Reloaded' Just Launched on a Network More Secret than Tor”, *Motherboard*, 11-1-2015. [en línea]. Disponible en: http://motherboard.vice.com/read/silk-road-reloaded-i2p.

[37] Silk Road (marketplace). [en línea]. Disponible en: https://en.wikipedia.org/wiki/Silk_Road_(marketplace).

[38] A. Greenberg. “New Dark-Web Market is Selling Zero-Day Exploits to Hackers”, *Wired*, 17-4-2015. [en línea]. Disponible en: http://www.wired.com/2015/04/therealdeal-zero-day-exploits.

[39] J. Cox. “The Mysterious Disappearance, and Reappearance, of a Dark Web Hacker Market”, *Motherboard*, 29-7-2015. [en línea]. Disponible en: http://motherboard.vice.com/read/the-mysterious-disappearance-and-reappearance-of-a-dark-web-hacker-market.

[40] "TheRealDeal Market", *DarkWebNews*, 31-5-2015. [en línea]. Disponible en: https://darkwebnews.com/darkwebmarkets/therealdeal-market.

[41] R. Dingledine, N. Mathewson y P. Syverson. “Tor: The Second Generation Onion Router”. En: Actas del Usenix Security Symposium, San Diego, CA, Estados Unidos, 2004. [en línea]. Disponible en: https://www.usenix.org/legacy/event/sec04/tech/full_papers/dingledine/dingledine_html/index.html.

[42] K. Zetter. "Tor Researcher Who Exposed Embassy E-mail Passwords Gets Raided by Swedish FBI and CIA", *Wired*, 14-11-2007. [en línea]. Disponible en: http://www.wired.com/2007/11/swedish-researc.

[43] D. McCoy, K. Bauer, D. Grunwald, T. Kohno y D. Sicker. “Shining light in dark places: Understanding the tor network”. En: Actas del 8th international symposium on Privacy Enhancing Technologies, Leuven, Bélgica, 2008. [en línea]. Disponible en: https://www.researchgate.net/publication/221655571_Shining_Light_in_Dark_Places_Understanding_the_Tor_Network.

[44] C. Soghoian. "Enforced Community Standards For Research on Users of the Tor Anonymity Network". En: Workshop on Ethics in Computer Security Research (WECSR), 2011. [en línea]. Disponible en: https://www.ifca.ai/pub/fc11/wecsr11/soghoian.pdf.

[45] N. Evans y C. Grothoff. “Deanonymizing Tor”. En: DEF CON 16, 2008. [en línea]. Disponible en: https://www.defcon.org/images/defcon-16/dc16-presentations/defcon-16-evans-grothoff.pdf.

[46] A. Biryukov, I. Pustogarov y R. Weinmann. "Trawling for Tor Hidden Services: Detection, Measurement, Deanonymization". En: Actas del IEEE Symposium on Security and Privacy, 2013 [en línea]. Disponible en: http://www.ieee-security.org/TC/SP2013/papers/4977a080.pdf.

[47] Y. Sun, A. Edmundson, L. Vanbever, O. Li, J. Rexford, M. Chiang y P. Mittal. “RAPTOR: Routing Attacks on Privacy in Tor”. Presentado a: *24th USENIX Security Symposium*, Washington, D.C., Estados Unidos, 2015 [en línea]. Disponible en: https://www.usenix.org/sites/default/files/sec15_full_proceedings.pdf.

[48] A. Kwon, M. AlSabah, D. Lazar, M. Dacier y S. Devadas. "Circuit Fingerprinting Attacks: Passive Deanonymization of Tor Hidden Services". Presentado a: 24th USENIX Security Symposium, Washington, D.C., Estados Unidos, 2015 [en línea]. Disponible en: https://www.usenix.org/sites/default/files/sec15_full_proceedings.pdf.

[49] "Russia offers $110,000 to crack Tor anonymous network", *BBC News*, 28-7-2014. [en línea]. Disponible en: http://www.bbc.com/news/technology-28526021.

[50] "OONI Explorer: Censorship and other Network Anomalies Around the World", *blog.torproject.org*, 23-3-2016. [en línea]. Disponible en: https://blog.torproject.org/category/tags/censorship [Consulta: 31 marzo 2016].

[51] FBI en español. [en línea]. Disponible en: https://www.fbi.gov/espanol. [Consulta: 31 marzo 2016].

[52] “Signals Intelligence”, *www.nsa.gov*, 3-5-2016. [en línea]. Disponible en: https://www.nsa.gov/what-we-do/signals-intelligence. [Consulta: 17 junio 2016].

[53] A. Peterson. "The NSA has its own team of elite hackers", *The Washington Post*, 29-8-2013. [en línea]. Disponible en: https://www.washingtonpost.com/news/the-switch/wp/2013/08/29/the-nsa-has-its-own-team-of-elite-hackers.

[54] "What we do", *GCHQ*. [en línea]. Disponible en: https://www.gchq.gov.uk/what-we-do [consulta: 17 junio 2016].
[55] Y. Levine. "Almost Everyone Involved in Developing Tor was (or is) Funded by the US Government", *Pando*, 16-7-2014. [en línea]. Disponible en: https://pando.com/2014/07/16/tor-spooks.
[56] "Tor black-market-related arrests", *gwern.net*, 14-7-2012. [en línea]. Disponible en: https://www.gwern.net/Black-market%20arrests [Consulta: 2 abril 2016].
[57] "Trip report: Tor trainings for the Dutch and Belgian police", *blog.torproject.org*, 5-2-2013. [en línea]. Disponible en: https://blog.torproject.org/blog/trip-report-tor-trainings-dutch-and-belgian-police.