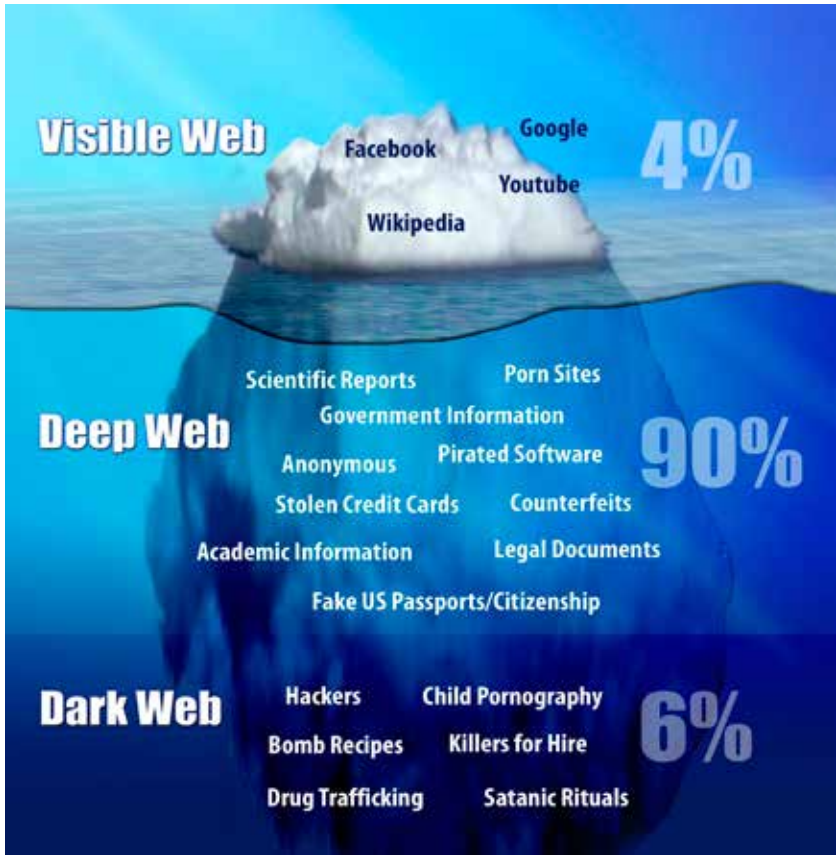
Web oculta 101

Mayor Jeremy Cole, USAF



Internet hoy tiene múltiples webs (redes). La web superficial/visible es lo que Google y otros motores de búsqueda indexan y leen en base a enlaces. En esencia, la web superficial es un índice maestro de índices de acceso público que proporciona resultados para búsquedas basadas en términos y enlaces. La web superficial es pequeña y representa solo el 4% del total. La segunda, llamada la web profunda o deep web, representa aproximadamente el 96% del resto de la web. La web profunda consiste de sitios protegidos que exigen que los usuarios introduzcan información para obtener acceso (correo electrónico o bancos en línea), contenido sin enlaces (blogs no publicados o bases de datos organizacionales), información protegida por derechos (resultados de estudios, registros financieros, investigación y desarrollo), e información personal (registros médicos o documentos legales. Todos éstos son parte de la web profunda. Los motores de búsqueda estándar no tienen acceso a estos sitios y por lo tanto no pueden buscar en ellos. La última es la web oculta o dark web, una parte de la web profunda. Para acceder a ella es necesario utilizar programas informáticos específicos, claves de acceso y conocimiento. Aquí se encuentran los sitios ocultos que prefieren permanecer en la oscuridad.

¿Qué tienen en común un hacker, una agencia de investigación del gobierno, EUROPOL, una fuente anónima que informa a un periodista, un disidente en un país donde se reprime la libertad de expresión, los traficantes de drogas, los pedófilos, los asesinos a sueldo, un denunciante de irregularidades, un fanático de la privacidad y los terroristas? Todos dependen del anonimato en línea para garantizar su privacidad, proteger la información personal, habilitar la libertad de expresión, o paradójicamente, para censurarla. Además, también confían del anonimato en línea para realizar actividades ilícitas. Sea para comunicarse, navegar en la web o alojar datos, estos individuos y organizaciones realizan sus actividades en la web oculta para permanecer ocultos de la vista del público. Qué es la web oculta, cómo funciona y quiénes son sus principales usuarios es esencial para entender que ella representa una mezcla de servicios ocultos que consiste de muchas personalidades diferentes provenientes de todos los segmentos de la sociedad.

¿Qué es?

Algunos conocen a la web oculta como "la parte sórdida de Internet donde se puede comprar drogas, armas, pornografía infantil, [y] contratar asesinos a sueldo".[1] Otros resaltan cómo "ayuda a los disidentes políticos que quieren evadir la censura del gobierno".[2] En cualquier caso, la web oculta es un grupo de sitios web difíciles de encontrar porque "no están indexados por los motores de búsqueda, como Google, y no se puede navegar fácilmente a ellos con un navegador estándar de web".[3] Un esbozo rápido de su desarrollo y evolución técnica define esta discusión. En un sentido general, la web oculta, también conocida como la red oculta, oculta la actividad en Internet de los individuos que la utilizan para comunicarse, alojar información o acceder a un sitio web específico. Tradicionalmente, el acceso a Internet depende de un proveedor de servicio Internet (ISP) que conecta los usuarios a Internet. Los ISP asignan direcciones IP (Protocolo Internet) a sus usuarios y máquinas anfitrionas. Las direcciones IP ofrecen detalles organizativos sobre el ISP, su ubicación geográfica, la ciudad más cercana, los sitios web visitados, y otras informaciones de identificación llamada metadatos. La web oculta permite que sus usuarios y máquinas anfitrionas naveguen por Internet, alojen un sitio web o se comuniquen de forma anónima usando una red global que confunde las direcciones IP de sus usuarios. Este concepto de anonimato se apoya en el software que el Laboratorio de Investigación Naval (NRL) de los Estados Unidos desarrolló en 2002. En 2004, el NRL publicó la segunda generación 'del encaminador cebolla (the onion router)' o Tor, como usualmente se le conoce. En mayo de 2004, Tor tenía "32 nodos (24 en Estados Unidos y 8 en Europa)".[4] Actualmente la red de Tor tiene más de 6000 nodos[5] siendo la más grande a nivel internacional y la herramienta principal usada para acceder a la web oculta.

Aunque el anonimato que Tor ofrecía a los usuarios de la red oculta era ventajoso, desde entonces la web oculta ha ganado otros usos–algunos legales, otros no. Por ejemplo, según uno de los desarrolladores originales de Tor, Michael Reed, las metas iniciales de Tor eran legítimas "Su *FINALIDAD* [sic] era para el uso del DoD [Departamento de Defensa de los EUA.] / Inteligencia…no para asistir a los disidentes…criminales [o] usuarios de bittorrent…".[6] Sin embargo, nueve años después del lanzamiento de su segunda generación, los investigadores de la Universidad de Luxemburgo evaluaron casi 40.000 sitios Tor ocultos. Como resultado, "encontraron que el contenido de los servicios ocultos de Tor era más bien diverso". El número de servicios ocultos con contenido ilegal o dedicados a actividades ilegales y el número de los otros servicios ocultos (dedicados a los derechos humanos, libertad de expresión, anonimato, seguridad,

¿Cómo se accede a la web oculta?

- Descargue un programa de anonimato (como Tor)
- Siga las instrucciones de instalación
- Inicie un navegador (debe conectarse automáticamente)
- Vaya a un directorio de servicios ocultos para comenzar (como el wiki Hidden)

etc.) es casi igual".[7] Curiosamente, los analistas encontraron una división numérica casi pareja entre sitios legítimos (56%) y sitios ilícitos (44%).[8] En vista del gran alcance de los nodos Tor a nivel mundial, parece justo afirmar que no todo es malo en la red oculta. El gobierno estadounidense invirtió aproximadamente 1,8 millones de dólares[9] en Tor en 2013. Hoy Tor es "un proyecto de código abierto operado por voluntarios y apoyado por activistas, organizaciones sin fines de lucro, universidades y gobiernos".[10] La combinación de estos factores sugiere que Tor y la web oculta en la que reside podría no estar tan plagada de crimen e ilegalidad como se pensaba anteriormente. A pesar de las opiniones divergentes, la web oculta existe para que los individuos, independientemente de las intenciones, puedan comunicarse, alojar datos o navegar en la web de forma anónima. Naturalmente, la web oculta y sus herramientas han evolucionado para incluir una amplia gama de actividad, pero sigue centrada en el anonimato.

¿Cómo funciona?

La web oculta utiliza programas de cifrado y anonimato para proteger a sus usuarios y máquinas anfitrionas. El uso del cifrado entre los usuarios de la web oculta no es nuevo. Por ejemplo, supuestamente el Estado Islámico de Irak y el Levante (ISIL) comenzó a experimentar con las herramientas de cifrado en noviembre de 2013.[11] Dos años después, la información posterior indica que el ISIL tiene ahora "un "servicio de asistencia" de 24 horas para asesorar al gran número de yihadistas en el cifrado de sus comunicaciones a fin de evadir a las autoridades".[12] Son escasos los informes de código abierto que contengan detalles sobre las técnicas de cifrado del ISIL, especialmente en lo relacionado a planes de ataque. Por ejemplo, inicialmente se creyó que el ISIL utilizó el cifrado para planear los ataques en París. Sin embargo, información posterior aclaró que la información sobre el planeamiento utilizando el cifrado de PlayStation4 era falsa.[13] En el último ataque motivado por el ISIL en San Bernardino, no hay información pública actual que indique que se haya utilizado cifrado en la planificación.[14] Sin embargo, según Aaron F. Brantly del Centro de Combate del Terrorismo afiliado con el Ejército de los Estados Unidos hay cuando menos "120 plataformas de [comunicación] separadas, muchas de ellas cifradas… que crean un espacio…para operar independientemente de la vigilancia directa".[15] Aunque estos ejemplos resaltan muchos usos negativos, el cifrado tiene un valor compensador al proteger todo lo que se hace en línea, desde pagar la factura de cable, administrar las finanzas, examinar los sitios web favoritos, comentar en los medios sociales, compartir opiniones importantes para uno, o escuchar la música favorita en línea. Debido a que el cifrado es esencial para proteger la autenticidad de la información personal y asegurar que solo personas autorizadas tengan acceso a ella, el software de anonimato continuará apoyándose en éste.

Fundamentalmente, la web oculta combina el cifrado con software de anonimato (SA)[16] para ocultar a sus usuarios y máquinas anfitrionas. Tor es el SA más común en la web oculta, aunque hay otras opciones como las redes privadas virtuales (VPNs), la comunicación entre pares "peer-to-peer" (P2P), o el Proyecto de Internet Invisible (I2P). Hay muchas técnicas para ocultar la identidad que utilizan un SA. Por ejemplo, Tor "cifra el tráfico web [el proceso 'dónde quiere ir en línea'] en capas y lo redirige a través de computadoras seleccionadas al azar entre los [6000 nodos disponibles referidos anteriormente] a nivel mundial, cada uno de estos elimina una sola capa de cifrado antes de transferir los datos al siguiente destino en la red".[17] Este proceso denominado 'salto' oculta al usuario de Tor y las direcciones IP de

¡Esté alerta!

- El acceso a los servicios y contenidos ilegales está a un clic de distancia.
- No se puede "negar haber visto" un contenido.
- Las representaciones de muerte violenta, muertes reales y suicidios son muy frecuentes.
- Pueden ocurrir impactos psicológicos.

la máquina anfitriona encaminándolos a través de tres puntos aleatorios[18] dificultando así la identificación del origen. Cuando se opera un sitio web mediante Tor, el IP del usuario y el servidor web saltan tres veces mientras que las VPN solo saltan una vez.[19] Otra técnica común denominada spoofing (burla)[20] crea la apariencia de que su IP está en algún otro lugar. Esto es bastante útil para ganar acceso a recursos en línea específicos (programas de televisión, compras, servicios de noticias, etc.) disponibles solo en un lugar físico dado que se basa en la dirección IP. Por ejemplo, mediante el uso de una VPN es posible acceder a Netflix, una empresa estadounidense, desde Italia utilizando un ISP italiano. Las VPN permiten que los clientes elijan direcciones IP en varios países habilitando el acceso a recursos en línea de forma anónima. Las VPN son bastante populares porque son "gratuitas y a menudo más rápidas que navegar por la red de Tor, y también son de más fácil uso".[21] El software de anonimato y el cifrado ofrecen a los usuarios y máquinas anfitrionas la capacidad de ocultar su identidad. Debido a que el cifrado garantiza el acceso autorizado solo a datos únicos, los usuarios de la web oculta confían en él. Cuando se combina el cifrado con software como Tor o una VPN que oculta la identidad del usuario, la probabilidad de mantenerse anónimo aumenta enormemente, protegiéndose así la identidad de los usuarios y las máquinas anfitrionas.

¿Quién la utiliza?

Ésta es una pregunta difícil de contestar ya que la mayoría de usuarios de la web oculta prefieren mantenerse anónimos. Sin embargo, considerando el número de usuarios de Internet, los sitios web disponibles, qué y cómo exploran los usuarios de la red oculta, el uso de la web oculta, que es infinitesimalmente pequeña, es una caja de sorpresas. Por ejemplo, actualmente hay más de 3 mil 200 millones de usuarios de Internet a nivel global[22] en comparación a lo que dice Tor que tiene 2 millones de usuarios diarios.[23] Suponiendo que los números de Tor son exactos; esto significa que el 0,0625% de los usuarios de Internet transitan por la web usando Tor. Es insensato concluir que los 2 millones utilizan Tor para acceder a la web oculta y vender drogas o buscar imágenes de abuso infantil. Los números de Tor indican que "solo el 1,5% del tráfico total... [tiene] que ver con los sitios ocultos".[24] Con cerca de mil millones[25] de sitios en línea, los estimados de Tor varían entre 7.000 y 30.000.[26] En otras palabras, la contribución de la web oculta de Tor es aproximadamente 0,03%[27] de la web global. Estos números sugieren una comunidad de usuarios, máquinas anfitrionas y datos disponibles en la web oculta muy pequeña. Según el proyecto Tor esta comunidad incluye "gente normal" interesada en protegerse de los "comerciantes inescrupulosos y ladrones de identidad...Reporteros sin fronteras, La Voz de América/Radio Europa Libre/Radio Asia Libre...Periodistas ciudadanos en China...Funcionarios del orden público...denunciantes de irregularidades...ejecutivos de empresas...blogueros...[y] militares...como agentes de campo, servicios ocultos y recopilación de inteligencia", entre otros".[28] Probablemente, estas personas utilicen la red oculta de Tor para proteger sus actividades en línea. Hay otros en la red oculta que el proyecto Tor no ha mencionado. Por ejemplo, hace dos años un individuo estableció un mercado para asesinar políticos a cambio de la moneda virtual bitcoin.[29] Otro ejemplo son los hackers que ofrecen sus servicios. Sin embargo,

Sitios comunes de la red oculta

Drogas: Brainmagic, Agora Phishing, Mom4Europe, Exit Seven, CocaineMarket, DreamMarket

Equipos: Hackintosh, TorGameDepot, Underground Electronics

Falsificaciones: USD Counterfeits, Cheap Euros, 20 Dollar USD Notes

Armas: European Arms, GlobalGuns, Black Market

Pasaportes: United States Citizenship, UK Passports

Otros: Rent-A-Hacker, Hitman Network, Bitcoin Financial, CloneCards, SocialHack, Silkroad Phishing

parece haber un problema porque "para establecer una relación comercial, los hacker deben ser corteses con sus clientes, completar sus tareas encubiertas de modo oportuno, y en algunos casos incluso ofrecer garantías de devolución del dinero".[30] Por el contrario, hay individuos bien intencionados como el hacker llamado 'Intangir', "quien se convirtió en defensor de la web oculta el pasado marzo de [2014] cuando pirateó la Wiki Hidden, y borró todos los enlaces a pornografía infantil".[31] Otro ejemplo es el Doctor X, un médico con experiencia que ayuda a la gente a reducir la dependencia en las drogas. El Doctor X estableció un sitio para ayudar a los usuarios del mercado de las drogas. Dijo que "la gente me pregunta sobre los riesgos reales y los efectos negativos, [de] las combinaciones de drogas [ilegales y con receta], y el uso de drogas por personas que sufren de diferentes condiciones, como diabetes o problemas neurológicos".[32] Estas acciones altruistas ofrecen la esperanza de que la decencia humana puede existir de forma anónima. En vista del pequeño número de usuarios de la red oculta y ofrecimientos en línea, la revisión de contenido popular para entender a los usuarios de la red oculta en base a los datos disponibles ofrece resultados mixtos. Por ejemplo, un informe de la Fundación de Vigilancia de Internet (IWF) encontró "31.266 URLs [localizador uniforme de recursos o enlace hacia un recurso en línea] que contenían imágenes de pornografía infantil".[33] De ellos, la IWF dijo "En 2014, identificamos 51 servicios ocultos no vistos anteriormente que distribuían contenido de abuso sexual infantil, un aumento de 55% en comparación al año 2013".[34] El contenido ilícito oculto, apenas un 0,002%, no es tan inquietante como el incremento en el uso de servicios ocultos para insertar contenido de abuso sexual infantil. Esto sugiere un aumento en las redes de abuso sexual infantil existentes en la red oculta. Un segundo ejemplo ilustra los hábitos de los vendedores de drogas en la red oculta. En noviembre de 2014, las autoridades legales y judiciales de 17 naciones[35] realizaron acciones para reprimir los mercados de drogas de la red oculta en una operación llamada 'Operación Onymous'. La operación produjo 17 arrestos, la confiscación de 414 dominios .onion [alojados por Tor], "más de 1 millón de dólares en bitcoins [dinero digital utilizado en línea sin ninguna participación institucional bancaria legítima], 250.000 dólares en efectivo",[36] otros activos y múltiples confiscaciones de mercados de drogas en línea. La operación se realizó con éxito, pero mientras que el "sitio de drogas más popular de la web oculta [Silk Road]",[37] quedó bloqueado, otros tomaron su lugar. Sitios como Agora prosperaron ofreciendo "más de 16.000 productos mayormente ilegales".[38] Avancemos seis meses y las cifras del 24 de abril de 2015 confirman que los sitios más pequeños del mercado de drogas de la red oculta "tuvieron un gran crecimiento con respecto al mes anterior".[39] Parece ser que el mercado de drogas actual se amplió gracias al vacío creado por la supresión del sitio web Silk Road. Esta actividad implica que los mercados de drogas continuaron y posiblemente hasta aumentaron su presencia en la red oculta después de Operación Onymous. Curiosamente, Agora, un mercado de drogas importante de la web oculta, cerró recientemente sus operaciones debido al temor de "que las vulnerabilidades en los servicios ocultos de Tor podrían dar lugar a que se localicen sus servidores".[40] En base a estos ejemplos y recordando las conclusiones del estudio de la Universidad de Luxemburgo antes mencionado, podemos concluir que la comunidad de la red oculta es pequeña, continúa impulsando la actividad ilegal a pesar de las continuas medidas enérgicas de los organismos del orden público y hace todo lo posible para evitar que la descubran utilizando las últimas tendencias tecnológicas.

Las tácticas de la red oculta varían, dificultando la identificación de usuarios o máquinas anfitrionas de la red oculta. Por ejemplo, el Dr. Gareth Owen, profesor de la Universidad de Portsmouth, al realizar un estudio de seis meses de los sitios ocultos de TOR encontró que el 75% de los usuarios de la web oculta visitaron sitios de abuso infantil. Sin embargo, Owen cuestionó los números debido a que "La mayoría de servicios ocultos solo fueron vistos una vez. Éstos tienden a existir por poco tiempo".[41] Los hallazgos de Owen confirman que una táctica básica de los sitios web ilícitos es reubicarse periódicamente. Lo que implica que el acceso continuo a estos sitios requiere contacto diligente y deliberado con la máquina anfitriona para obtener la última ubica-

ción del sitio real. Otra táctica común es usar sitios falsos, o fraudulentos. El no saber qué sitios son reales y cuales son falsos, complica los esfuerzos de vigilancia. Por ejemplo, un informe sobre la Operación Onymous alega que casi la mitad de los sitios incautados y cerrados eran falsos o fraudulentos".[42] Así, esta táctica ofrece a los usuarios de la red oculta protección en un entorno donde uno "podría estar a un clic de distancia de sitios que venden drogas y armas, y -francamente- incluso cosas peores".[43] Otra táctica, usar las VPN en un entorno donde reina la censura, permite la comunicación en la red oculta. Un bloguero chino que estableció una red oculta dijo "Este es un mundo Internet Chino libre, aquí puedes decir lo que piensas".[44] Otro respondió con entusiasmo a la publicación diciendo "me siento nervioso incluso ahora, a causa de mi personalidad tímida. Nunca pensé que mi primer contacto con la web oculta sería en un sitio web chino. Espero que el webmaster continúe su buena labor".[45] Estas tácticas reflejan las preocupaciones de los usuarios en proteger su identidad para evitar ser descubiertos haciendo algo ilícito o considerado ilegal. Para resumir, los números muestran que en general la comunidad de la web oculta –usuarios y sitios ofrecidos– es apenas una gota en el gran cubo de "Internet". La evaluación de las visitas a los sitios web ofrece muy poco para ayudar a definir a los usuarios de la red oculta y produce resultados mixtos debido a las tácticas que enmascaran la actividad.

Hitman Network: Somos un equipo de 3 asesinos a sueldo que trabajan en los EUA (+ Canadá) y en la UE. Una vez que usted hizo una compra le responderemos en un plazo de 1-2 días, y el contrato se completará dentro de 1-3 semanas dependiendo del blanco. Única Regla: no niños menores de 16 años y no políticos entre los 10 superiores

Aumentar el conocimiento de la web oculta y de cómo funciona no es tan difícil como definir quiénes forman la comunidad de la red oculta. Originalmente, la red oculta servía fines legítimos del gobierno de los Estados Unidos, proporcionando protección a los individuos que realizaban investigaciones, trabajo de campo y recopilación de inteligencia. Sin embargo, los individuos que buscaban sacar partido de la actividad criminal hicieron posible que la red oculta prosperara usando principalmente Tor. Curiosamente, los diseñadores de Tor esperaban que esto sucediera, mencionando que "habrá otros usos inevitables de la tecnología...y si esos usos fueran a darnos más tráfico de cobertura para ocultar mejor el uso que deseamos hacer de la red, tanto mejor".[46] La red oculta depende del cifrado y el anonimato para proteger a los usuarios y máquinas anfitrionas. El cifrado de datos es un antiguo estándar dorado de protección que garantiza que solo los individuos autorizados obtengan acceso a información verificable, no modificada. El uso del software de anonimato junto con el cifrado ofrece una protección compleja y

potente a la comunidad de la web oculta. En comparación con el número agregado de usuarios de Internet, los usuarios de la red oculta son casi inexistentes. Además, el número de sitios web de la red oculta disponibles comparado con los sitios web normales es mínimo –aproximadamente lo que sería un electrón en la cabeza de un alfiler en la mano de un jugador de baloncesto parado a media cancha en el Alamodome en San Antonio, Texas. Dada la naturaleza de la web oculta, es difícil definir quiénes son sus usuarios. La información disponible sugiere que unos cuantos tipos de usuarios: expertos en informática cuyas tácticas les ayudan a evitar los enredos legales, expertos en informática motivados por altruismo y usuarios normales que simplemente se interesan en proteger su información personal. En el mundo global interconectado de hoy, es más probable que la comunidad de la red oculta siga aumentando su popularidad como reflejo de una sociedad de enigmas legales y morales que aparentemente nadie en particular ha descifrado. ❑

Notas

1. http://blog.dictionary.com/dark-web/, consultado el 25 de noviembre de 2015.
2. http://www.npr.org/sections/alltechconsidered/2014/05/25/315821415/going-dark-the-internet-behind-the-internet,%20accessed%2030%20November%202015, consultado el 2 de diciembre de 2015.
3. http://www.ibtimes.co.uk/ukraine-combatants-turn-dark-web-advice-bridge-bombing-anti-tank-missiles-1487256, consultado el 2 de diciembre de 2015.
4. Dingledine, Roger., Mathewson, Nick., & Syverson, Paul. Tor: The Second-Generation Onion Router (Tor: El Encaminador Cebolla de Segunda Generación), Número de publicación NRL 03-1221.1-2602, página 13.
5. http://www.wired.com/2015/09/mapping-tors-anonymity-network-spread-around-world/, consultado el 12 de diciembre de 2015.
6. https://cryptome.org/0003/tor-spy.htm, consultado el 10 de diciembre de 2015.
7. Biryukov, Alex., Philipp Weinmann, Ralf. y Pustoarov, Ivan. Content and popularity analysis of Tor hidden services (Análisis del contenido y la popularidad de los servicios ocultos de Tor), 29 de julio de 2013.
8. Ibíd.
9. http://www.independent.co.uk/voices/comment/the-dark-web-is-not-just-for-paedophiles-drug-dealers-and-terrorists-9920667.html, consultado el 14 de diciembre de 2015.
10. http://f3magazine.unicri.it/?p=889, consultado el 14 de diciembre de 2015.
11. http://www.thedailybeast.com/articles/2014/11/13/isis-keeps-getting-better-at-dodging-u-s-spies.html, consultado el 4 de diciembre de 2015.
12. http://thehill.com/policy/cybersecurity/260402-isis-help-desk-aides-would-be-terrorists-with-encryption, consultado el 8 de diciembre de 2015.
13. https://www.washingtonpost.com/news/the-intersect/wp/2015/11/16/everything-the-internet-hoax-machine-tricked-you-into-believing-about-paris/, consultado el 3 de diciembre de 2015.
14. http://www.ibtimes.com/obama-couldnt-stop-san-bernardino-shooters-expect-more-isis-details-sunday-speech-2213315, consultado el 7 de diciembre de 2015.
15. http://www.nbcnews.com/storyline/paris-terror-attacks/are-isis-geeks-using-phone-apps-encryption-spread-terror-n464131, consultado el 8 de diciembre de 2015.
16. http://www.wired.com/2014/11/hacker-lexicon-whats-dark-web/, consultado el 25 de noviembre de 2015.
17. Ibíd.
18. Ibíd.
19. http://motherboard.vice.com/read/what-firewall-chinas-fledgling-deep-web-community, consultado el 2 de diciembre de 2015.
20. http://www.pcadvisor.co.uk/how-to/internet/what-is-dark-web-how-access-dark-web-deep-joc-3593569/, consultado el 2 de diciembre de 2015.
21. http://motherboard.vice.com/read/what-firewall-chinas-fledgling-deep-web-community, consultado el 2 de diciembre de 2015.22. Cole-Dark Web 101 final_spa.docxconsultado el 9 de diciembre de 2015.22. http://www.wired.com/2015/06/dark-web-know-myth/ consultado el 9 de diciembre de 2015.
22. Cole-Dark Web 101 final_spa.docxconsultado el 9 de diciembre de 2015.
23. http://www.wired.com/2015/06/dark-web-know-myth/, consultado el 9 de diciembre de 2015.
24. Ibíd.
25. http://www.internetlivestats.com/total-number-of-websites/, consultado el 12 de diciembre de 2015.
26. Ibíd.
27. Ibíd.
28. https://www.torproject.org/about/torusers.html.en, consultado el 11 de diciembre de 2015.29.
29. http://www.forbes.com/sites/andgreengberg/2013/11/18/meet-the-assassination-market-creator-whoscrowdfunding-murder-with-bitcoins/, consultado el 11 de diciembre de 2015.

30. http://www.ibtime.co.uk/new-breed-lone-wolf-hackers-are-roaming-deep-web-their-prey-getting-bigger-1483347 consultado el 11 de diciembre de 2015.
31. http://www.ibtime.co.uk/how/cyber-vigilantes-catch-paedophiles-terrorist-lurking-deep-web-1479291, consulatdo el 11 de diciembre de 2015.
32. Ibíd.
33. https://www.iwf.org.uk/assets/media/annual-reports/IWF_Annual_report_14_web.pdf página 9, consultado el 10 de diciembre de 2015
34. Ibíd, página 17.
35. https://www.europol.europa.eu/content/global-action-against-dark-markets-tor-network, consultado el 2 de diciembre de 2015.
36. http//www.wired.com/2014/11operation-onymous-dark-web-arrest/, consultado el 10 de diciembre de 2015.
37. http://www.wired.com/2014/11/feds-seize-silk-road-2/, consultado el 15 de diciembre de 2015.
38. Ibíd.
39. http://www.digitalcitizensalliance.org/cac/alliance/content.aspx?page=Darknet, consultado el 11 de diciembre de 2015.
40. http://www.scmagazine.com/dark-website-agora-closes-over-tor-vulnerability-suspicions/article/435278/, consultado el 15 de diciembre de 2015.
41. http://www.bbc.com/2014/11/18/nearly-half-of-the-operation-onymous-takedowns-were-scam-or-clone-sites/ consultado el 12 de diciembre de 2015.
42. http://techcrunch.com/2014/11/18/nearly-half-of-the-operation-onymous-takedowns-were-scam-or-clone-sites/, consultado el 12 de diciembre de 2015.
43. http://www.pcadvisor.co.uk/how-to/internet/what-is-dark-web-how-access-dark-web-deep-joc-3593569/, consultado el 16 de diciembre de 2015.
44. http://motherboard.vice.com/read/what-firewall-chinas-fledgling-deep-web-community consultado el 2 de diciembre de 2015.
45. Ibíd.
46. https://cryptome.org/0003/tor-spy.htm, consultado el 10 de diciembre de 2015.

"Las opiniones expresadas en este artículo son las del autor y no reflejan necesariamente la política oficial o la posición de la Fuerza Aérea, el Departamento de Defensa, o el Gobierno EE.UU."

Mayor Jeremy Cole, USAF (Licenciatura en Español, Weber State University, Maestría en Español University of Kansas) es actualmente Director de Curso en la eSchool of Graduate PME en Maxwell AFB, AL. Como oficial de carrera de inteligencia, ha trabajado en múltiples niveles incluyendo el Comando Combatiente.

DARPA

Al hacer una simple búsqueda en Internet sobre un tema, los resultados que aparecen no son toda la historia. El Internet contiene un vasto tesoro de información - a veces llamado la "Web profunda" - que no está indexado por los motores de búsqueda: información que sería útil para el seguimiento de los criminales, actividades terroristas, el tráfico sexual y la propagación de enfermedades. Los científicos también podrían utilizarlo para buscar imágenes y datos de las naves espaciales. La Agencia de Proyectos de Investigación Avanzada de Defensa (DARPA) ha estado desarrollando herramientas como parte de su programa de Memex que accesa y cataloga el mundo misterioso de la Web profunda. Los investigadores en el Laboratorio de Propulsión a Chorro de la NASA en Pasadena, California, se han unido al esfuerzo Memex para aprovechar los beneficios de la Web profunda en busca de la ciencia. Memex podría, por ejemplo, ayudar a catalogar la enorme cantidad de datos que las naves espaciales de NASA entregar a diario.

Elizabeth Landau
Jet Propulsion Laboratory, Pasadena, California.