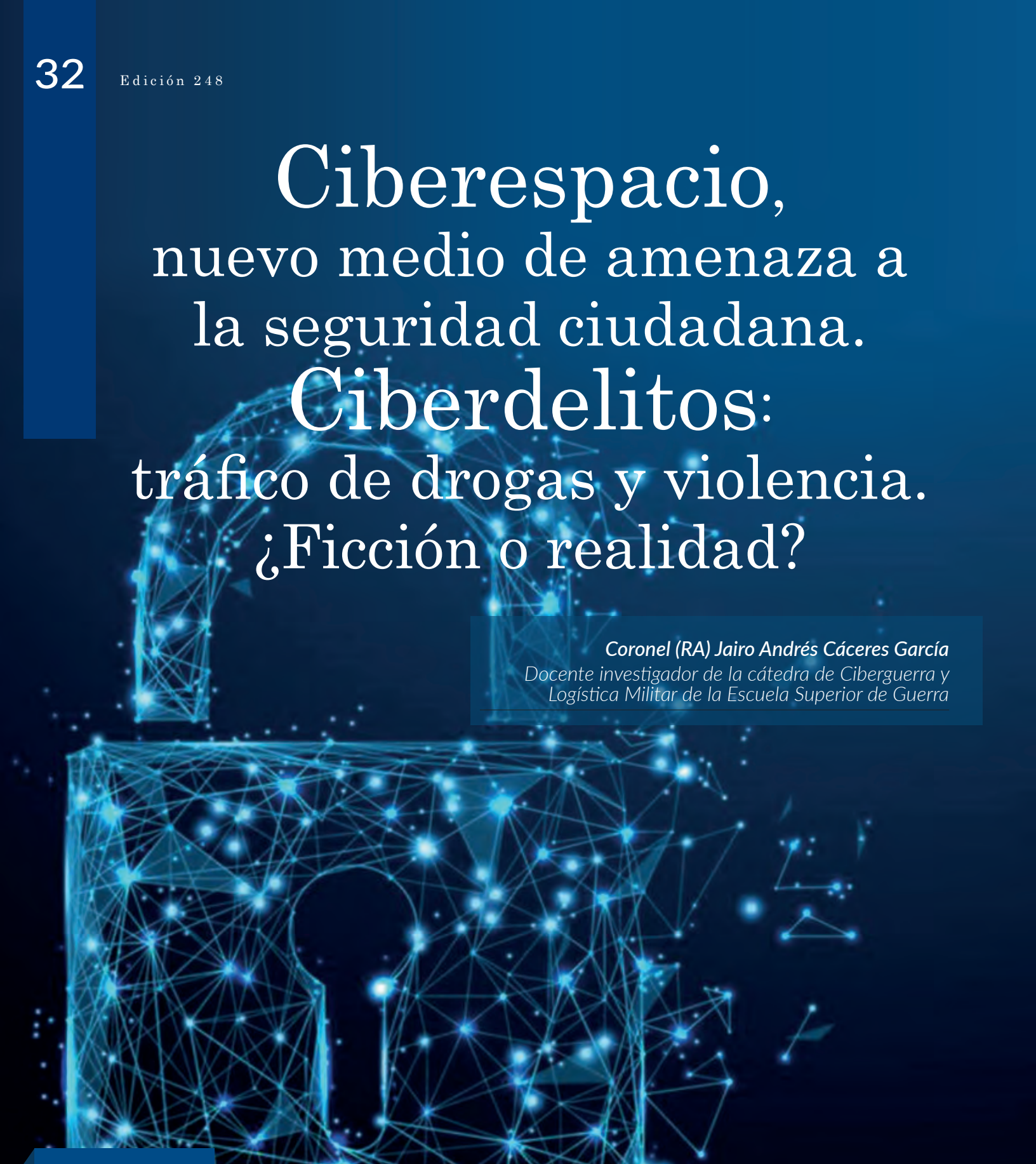
Ciberespacio, nuevo medio de amenaza a la seguridad ciudadana. Ciberdelitos: tráfico de drogas y violencia. ¿Ficción o realidad?

Coronel (RA) Jairo Andrés Cáceres García
Docente investigador de la cátedra de Ciberguerra y Logística Militar de la Escuela Superior de Guerra



Coronel
de la Reserva Activa
Jairo Andrés
Cáceres García

Docente investigador de la cátedra de Ciberguerra y Logística Militar de la Escuela Superior de Guerra "General Rafael Reyes Prieto", de Bogotá (Colombia). Magíster en Informática, de la Universidad Autónoma de Guadalajara (México). Magíster en Ingeniería en Sistemas Logísticos, de la Pontificia Universidad Católica de Valparaíso (Chile) en conjunto con la Academia Politécnica Militar (Chile). Diplomado de Alta Dirección en Seguridad Privada, de la Universidad Sergio Arboleda (Colombia). Diplomado Seguridad Informática, de la Universidad de Alcalá (España).

Foto: https://www.momentogp.com/wp-content/uploads/2019/02/cyber-2.png

Introducción

A partir de la década de 1990, el sistema internacional ha sido testigo de un fenómeno multidimensional, dinámico y complejo que ha generado transformaciones de manera impactante en todas las esferas de la vida del ser humano: la globalización. La desregulación de la economía, la apertura de mercados y el incremento exponencial del flujo de bienes y servicios y de personas a escala transnacional han estimulado el crecimiento y el desarrollo de los Estados, no solo en el ámbito económico, sino también en los espacios social, político y cultural.

Lo anterior ha facilitado el surgimiento de una plétora de nuevas tecnologías, propiciada por la llamada Revolución Tecnológica, la cual ha permitido la convergencia para la innovación del procesamiento del conocimiento y la aplicación de dos elementos muy importantes: la información y la comunicación. Así, las tecnologías de la información y la comunicación (TIC) han coadyuvado al relacionamiento entre personas desde cualquier parte del mundo, no importa a cuántos kilómetros de distancia se encuentren, gracias a la potenciación y la intensificación de herramientas que ya existían, como el internet.

El internet ha sido muy importante, pues ha ayudado a la expansión de las redes de conectividad entre personas, empresas, gobiernos, y las bases existentes de conocimiento, gracias a las innumerables motores de búsqueda que remiten al usuario a cualquier sitio web que se quiera consultar, y acceder a una gran cantidad de bienes y servicios: desde alimentos, vestuario y tiquetes para viajes hasta programas universitarios, vehículos de alta gama y acciones en la bolsa de valores y de cualquier empresa.

De internet se genera un concepto que, en la mayoría de los casos, suele ser empleado de manera intercambiable: el ciberespacio. Este se caracteriza por ser una construcción digital de servidores, computadores conectados entre sí, que permiten recibir y enviar información. Y no se trata de un ámbito físico, que pueda ser tocado.

No obstante lo anterior, ni la difusión de nuevas tecnologías ni las virtudes de internet han sido empleadas únicamente para el bien. La creación de este escenario virtual e intangible ha comportado la inclusión de una nueva problemática: el ciberdelito. La excepcionalidad de las propiedades del ciberespacio permite que los criminales actúen en él sin ser identificados ni reconocidos por las autoridades; es decir, bajo el anonimato, pues en el ciberespacio no hay banderas, uniformes ni jurisdicciones.

En este sentido, el ciberespacio ofrece un espacio para el ejercicio del ciberdelito y, adicionalmente, el crimen transnacional organizado (CTO), problemáticas que han sido potenciadas gracias al internet y a una dimensión más bien desconocida, pero muy compleja y peligrosa: la *darkweb*, en cuyas profundidades es posible advertir toda una serie de mercados ilegales para el cibercrimen, como el tráfico de drogas y de armas, el fraude y las falsificaciones de documentos, el lavado de dinero y la trata de personas, además de la promoción y la publicidad de grupos terroristas en todo el mundo.

Este artículo inicia explicando el impacto de la globalización en la emergencia de nuevas herramientas como el internet y el ciberespacio. En segundo lugar, se expone el fenómeno del ciberespacio, su importancia y sus implicaciones. Posteriormente, se explica cómo el ciberespacio ha dado lugar a ciberdelitos gracias a nuevos dominios del internet, como la *deepweb* y la *darkweb*. Por último, se ofrecen unas recomendaciones para hacer frente a esta amenaza que afecta la seguridad y defensa nacionales, y se concluye.

1. La globalización como origen del ciberespacio

Con el fin de la Guerra Fría, el mundo ha podido presenciar la intensificación de un fenómeno que, si bien ya existía, ha adquirido mayor fuerza con el colapso del comunismo en el Bloque Oriental: la globalización. Este fenómeno, de carácter multidimensional, complejo y dinámico,

se ha expandido y ha facilitado no solo el movimiento de las personas, sino también, el flujo de bienes, servicios y capital (Petcu, 2017), a lo largo de las fronteras nacionales a lo largo y ancho del globo. La eliminación de las restricciones al comercio y las finanzas internacionales, la desregulación de las economías y la liberación de los mercados han incrementado el comercio global y estimulado el crecimiento de economías nuevas y libres y el movimiento transfronterizo de bienes, personas y capital (INCB, 2001). La exportación de trabajos de países más desarrollados a países menos desarrollados, junto con los avances recientes en agricultura y el acceso a alimentación, medicinas, salud y educación, han sido efectos positivos de la globalización (Petcu, 2017).

Así mismo, la globalización ha facilitado el desarrollo de la ciencia y la tecnología, al mejorar las condiciones preexistentes para la comunicación y el relacionamiento entre personas, organizaciones y Estados, al omitir las fronteras y al llegar a, virtualmente, cualquier rincón del planeta. La Revolución Tecnológica ha favorecido la convergencia en su núcleo de dos aspectos para la innovación del procesamiento del conocimiento y su aplicación: la información y la comunicación (Castell, 1997).

En este sentido, el surgimiento de las tecnologías de la información y la comunicación (TIC) ha trasformado de manera significativa el diario vivir de todos los seres humanos, gracias a la maximización y la potenciación de herramientas preexistentes, como los teléfonos móviles, los computadores y el internet (Arbeláez, 2014). Respecto a este último, es posible afirmar que el internet ha reducido los espacios y los tiempos entre los usuarios, al permitir la expansión de las comunicaciones y el acceso a un innumerable conjunto de aplicaciones virtuales que permiten la expansión del conocimiento (Fazio, 2001) y la adquisición de nuevas habilidades y productos, gracias a portales cuya búsqueda remite a sitios web de, prácticamente, cualquier temática deseada: alimentos, vehículos, vestuario, vivienda, entretenimiento, viajes, finca raíz, propiedades, educación, finanzas y todo tipo de mercados y negocios.

2. El ciberespacio

El internet ha dado origen a un concepto que, en muchos casos, suele ser empleado de manera intercambiable o para hacer referencia al mismo escenario: el ciberespacio. De acuerdo con el Consejo Nacional de Política Económica y Social de la República de Colombia (CONPES, 2011), en virtud de la Resolución CRC 2258 de 2009, el ciberespacio puede ser definido como "el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (*software*), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios" (p. 38).

Para Kuehl (2009), el ciberespacio se entiende como "un dominio caracterizado por el uso de la electrónica y el espectro electromagnético para almacenar, modificar e intercambiar información a través de redes sistemas de información e infraestructuras físicas" (capítulo II).

En otras palabras, el ciberespacio es una realidad virtual, una construcción digital de servidores, computadores conectados entre sí, que permite recibir y enviar información. No se trata de un ámbito físico, tangible, que pueda ser tocado.

La aparición de este escenario ha supuesto la convergencia de múltiples actores ubicados en todos los lugares del mundo, quienes cuentan con la facultad de actuar libremente y fuera de cualquier circunscripción legal o normativa, sin restricciones ni limitaciones, y así desafiar el control del Estado (Larochelle, 2004) y de entes de vigilancia y de supervisión jurídica. En tal sentido, el ciberespacio puede comprenderse como un mundo gris, tenebroso y oscuro, en el que la seguridad no siempre está garantizada. En el ciberespacio no vemos banderas, ni uniformes ni jurisdicciones, no le vemos la cara al enemigo, pues este opera bajo un manto de anonimato.

De esa manera, es posible afirmar que el campo de batalla mundial está migrando de los cuatro

dominios tradicionales al quinto dominio (figura 1). Además de tierra, mar, aire y espacio, el ciberespacio ha conseguido constituirse como el nuevo teatro de la guerra, de quinta generación, vinculado con la existencia de la guerra híbrida (Gaitán, 2012).

Por su carácter transnacional, que desconoce fronteras y actúa indiscriminadamente a lo largo de los territorios nacionales, y gracias a ello desafía cualquier jurisdicción y todo control estatal, el ciberespacio ha permitido el origen de una nueva problemática: el ciberdelito.

El *ciberdelito* es definido por el CONPES 3701 (2011) como una "actividad delictiva o abusiva relacionada con los ordenadores y las redes de comunicaciones, bien porque se utilice el ordenador como herramienta del delito, bien porque sea el sistema informático (o sus datos) el objetivo del delito".

Entre los ciberdelitos más destacados, es posible encontrar: la guerra informática, los ciberataques, el ciberterrorismo, la infracción de derechos de autor, el fraude de identidad y el robo de información, la ciberextorsión y el tráfico de armas, identidades, drogas y personas, potenciados todos ellos por el CTO, sobre lo cual hablaremos más adelante.

2.1. La ciberseguridad

Para hacer frente a los ciberdelitos, los Estados han recurrido a la inclusión de la política de la Ciberseguridad dentro de sus lineamientos de seguridad y defensa nacionales. El CONPES 3701 (2011) de Colombia define la *ciberseguridad* como la "capacidad de un Estado para minimizar el nivel de riesgo al que están expuestos sus ciudadanos, ante amenazas o incidentes de naturaleza cibernética".

Es importante tomar en cuenta, en esta definición, la palabra "minimizar", ya que el Estado hace lo que le corresponde y lo que está a su alcance, de acuerdo con sus facultades y sus capacidades, pero hacerlo no es toda su responsabilidad, considerando, además, que dichas amenazas cibernéticas son difíciles de supervisar, vigilar y controlar, dado el carácter especial, cuasi invisible y sigiloso del ciberespacio, en el cual se puede desarrollar una numerosa cantidad de actividades

Figura 1. Los cinco dominios de la guerra
Fuente: elaboración propia, adaptado de Gaitán (2012).

La difusión de nuevas tecnologías y las virtudes del internet no han sido empleados únicamente para el bien. La creación de este escenario virtual e intangible ha comportado la inclusión de una nueva problemática: el ciberdelito.

ilegales, como el terrorismo, el tráfico de armas y el narcotráfico, entre otros. Al respecto, es pertinente cuestionarse por qué algunos criminales deciden actuar en el ciberespacio.

2.2. ¿Por qué migran los delincuentes al ciberespacio?

- En primer lugar, no hay que estar en sitio ni exponer la vida. Por ejemplo, los traficantes de drogas pueden trabajar a distancia para orquestar y dirigir las rutas del narcotráfico, las estrategias de envío, la producción, la recepción y la logística en general, y así evadir en el proceso la persecución de las autoridades y evitarse exponer su vida, su identidad y su integridad (Cooper & Akino, 2015).
- En segundo lugar, la velocidad del ilícito es mayor que la posible en las operaciones tradicionales, dadas la rapidez y la facilidad de las tecnologías para coordinar envíos de drogas y armas a distintas regiones del mundo, al alcance de un computador o un dispositivo electrónico (Cooper & Akino, 2015).
- En tercer lugar, el anonimato y la indetectabilidad garantizan a los delincuentes una protección ante los mecanismos del Estado para perseguirlos y localizarlos. Gracias a la tecnología tan avanzada de hoy, es posible emitir y recibir señales, llamadas y comunicaciones a través de dispositivos que no permiten el rastreo ni la geolocalización, lo cual facilita a los delincuentes interactuar sin ser descubiertos (Cooper & Akino, 2015).
- En cuarto lugar, está la criptomoneda, una moneda digital producida por una red pública, en vez de por un gobierno, y que utiliza la criptografía para asegurar que los pagos se envíen y se reciban de forma segura (Cooper & Akino, 2015).

Todos estos beneficios del ciberespacio para cometer delitos nos remiten al siguiente apartado.

3. ¿Ciberespacio: ¿un "nuevo" medio para tráfico de drogas y ciberdelitos?

El ciberespacio ha dado lugar a varias capas de redes; unas, legales, y otras, ilegales. Por tal motivo, es importante mencionar y establecer las diferencias que existen entre una y otra, para no entrar en confusiones. Estas capas de la red pueden ser ejemplificadas con un iceberg: la primera porción del internet, la *World Wide Web* (www), está disponible para todos, es accesible con buscadores convencionales. A medida que vamos descendiendo en el iceberg, vamos encontrando porciones más oscuras y profundas del internet: la *deep web* (red profunda) y la *dark web* (red oscura) (figura 2).

3.1. *World Wide Web* (web)

En primer lugar, está la porción del internet que es más familiar para todos nosotros: la www. Todos tenemos acceso a ella y hace parte de nuestro diario vivir virtual. Para ingresar a ella, es posible hacer uso de varios navegadores conocidos (Google Chrome, Internet Explorer, Firefox), los cuales nos dirigen a una gran cantidad de contenidos, incluyendo redes sociales (Facebook, Twitter, Instagram, YouTube), páginas de entretenimiento, comerciales, informativas, gubernamentales, educativas, etc. En la www podemos encontrar, básicamente, cualquier información que deseemos (Gallardo, 2017).

> Colombia define la ciberseguridad como la "capacidad de un Estado para minimizar el nivel de riesgo al que están expuestos sus ciudadanos, ante amenazas o incidentes de naturaleza cibernética."

3.2. *Deep web* (red profunda)

Esta hace referencia a una clase de contenido que no puede ser accedido por motores de búsqueda tradicionales, pues dicho contenido ha sido deliberadamente no indexado. Para ingresar a ella, se requieren permisos y claves especiales (Finklea, 2017). Se considera que el 96% de todo el contenido del internet se encuentra, precisamente, en esta porción de la red. Con más de 7500 terabytes de contenido, en la *deep web* se pueden encontrar *software* privados, archivos de web, websites indexadas, redes P2P, contenido dinámico, contenido encriptado y contenido no-HTML, entre otros (Cooper & Chikada, 2015).

El primer antecedente de esta red profunda se remonta a la creación de la "Silk Road", el primer mercado negro *online*, creado por Ross Ulbricht, y en el cual los usuarios podían encontrar todo tipo de productos de contrabando, principalmente drogas ilegales, hasta que fue desmantelada por el FBI en 2013 (Sui, Caverlee & Rudesill, 2015). Este tipo de mercados negros abriría paso a más modernos y contemporáneos mercados oscuros, cuyo modelo de compras es similar al de páginas como EBay o Amazon, donde se pueden encontrar catálogos de compras y carritos de compras para adquirir estos productos ilegales.

3.3 *Dark Web* (red oscura)

Finalmente, encontramos la zona más profunda: la red oscura. Al igual que la red profunda, la *dark web* no puede ser accedida por motores de búsqueda tradicionales, toda vez que su contenido se encuentra deliberadamente oculto.

A ella se puede acceder a través de una red conocida como TOR (The Onion Router). Inicialmente, TOR fue creado en 2002 por el US Naval Research Laboratory, como una herramienta para comunicarse *online* de manera anónima (Sui, Caverlee & Rudesill, 2015). Sin embargo, con el transcurso de los años, esta propiedad de anonimato e indetectabilidad ha sido aprovechada por criminales y terroristas para coordinar acciones y conversaciones a través de esta red oscura.

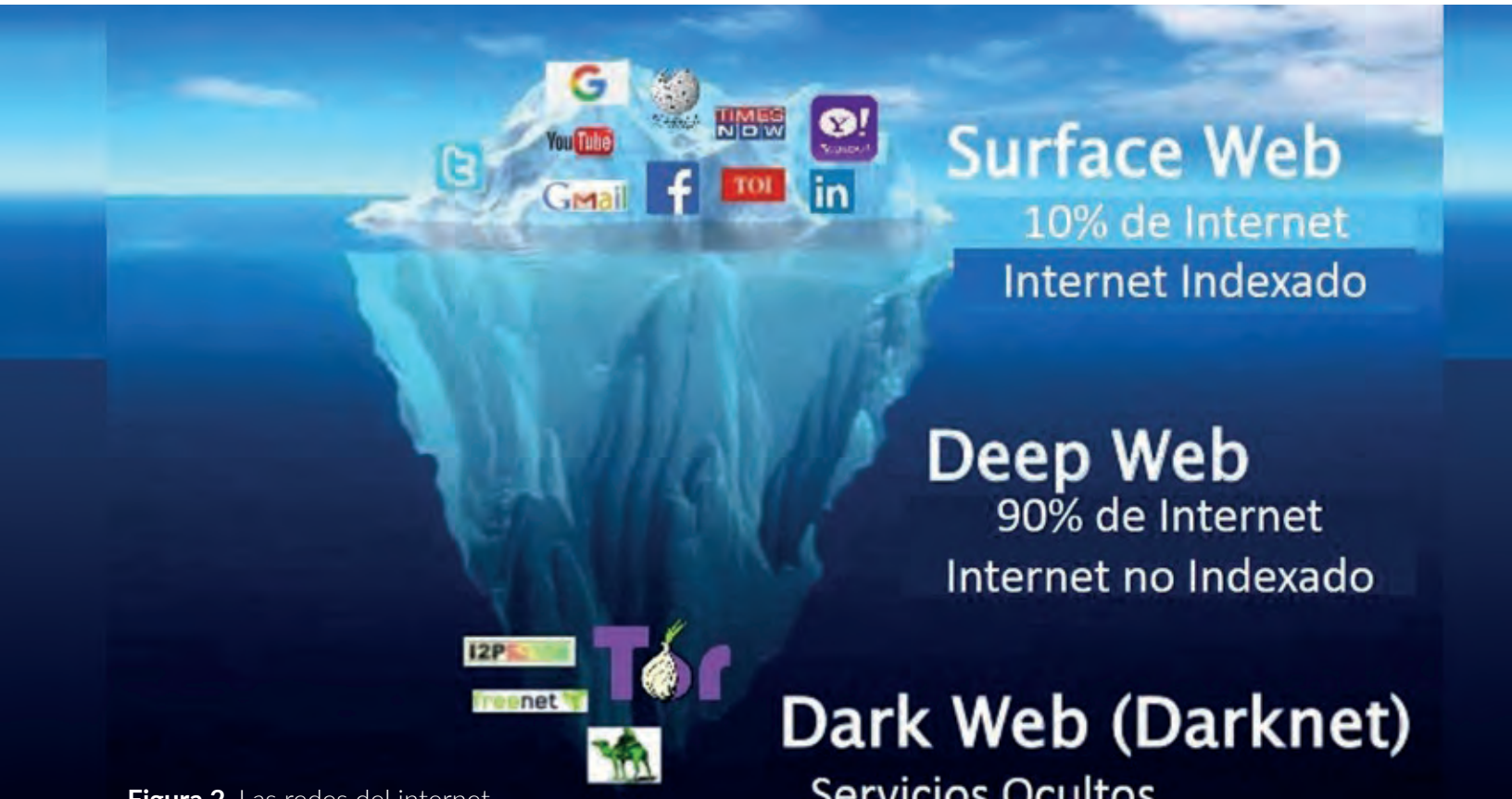
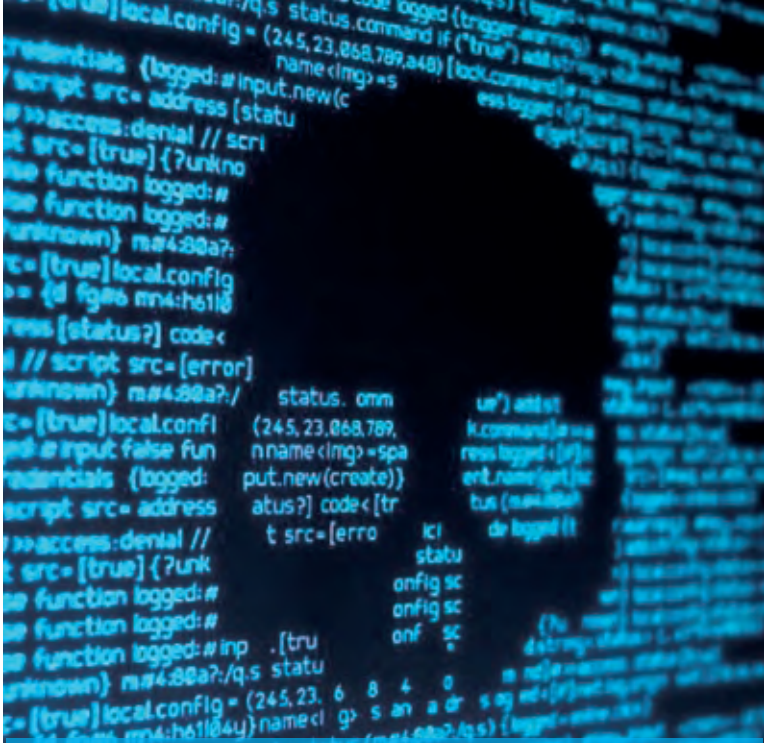


Figura 2. Las redes del internet
Fuente: www.diariopopular.com.ar/tecnologia/como-es-la-deep-web-la-red-donde-se-movia-el-pediatra-del-garraham-detenido-pornografia-infantil-n398138

Los criminales aprovechan la excepcionalidad del anonimato de la red oscura; sus actividades son indetectables, y los recursos, invisibles (Cooper & Chikada, 2015). Por tal motivo, la red oscura ha sido utilizada para la comisión de delitos y acceso a recursos de todo tipo de magnitud y nivel (Gallardo, 2017):

- ***Financiero:*** lavado de *bitcoins*, cuentas robadas de PayPal, tarjetas de crédito clonadas y prepagadas, falsificación de dinero.
- ***Comercial:*** explotación sexual, mercado negro, *gadgets* robados, armas y municiones, falsificación de documentos, venta de drogas, medicamentos, *software*.
- ***Anonimato y seguridad:*** instrucciones para reforzar la seguridad del acceso; acceso a mercado negro de sicarios.
- ***Servicio de*** hosting***:*** sitios de alojamiento con absoluta privacidad.
- ***Blogs, foros y tablones de imágenes:*** compraventas, *hacking* e intercambio de imágenes; foros de *crackers* en busca de víctimas.
- ***Servicio de correo y mensajería:*** gratis y de pago con SSL y soporte de IMAP. Los chats sobre IRC o XMPP.
- ***Activismo político:*** archivos censurados, hacktivismo y anarquía; documentos clasificados.
- ***Secretos de Estado y soplones:*** un *mirror* de WikiLeaks y lugares para publicar.



Fotos: https://expansion.mx/tecnologia/2018/10/01/el-cibercrimen-pasara-factura-por-600-000-mdd-de-dolares-a-nivel-mundial

- ***Libros:*** miles de *e-books* libres de *copyright* y en distintos formatos, así como descargas ilegales.
- ***Páginas eróticas:*** pornografía de pago y libre acceso, sin límite moral.
- Hackeo ***por encargo:*** Ataques DDoS, troyanos, *phishing*, *spamming*, *botnet agents*.

REFERENCIAS

Arbeláez, M. (2014). Las tecnologías de la información y la comunicación (TIC) un instrumento para la investigación. *Investigaciones Andina, 16*(29). Recuperado de http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0124-81462014000200001&lng=en&tlng=es.

Castells, M. (1997). *La era de la información: Economía, sociedad y cultura*. Madrid: Alianza Editorial.

Cooper, E., & Chikada, A. (2015). *The Deep Web, the Darknet, and Bitcoin.* Recuperado de https://www.markmonitor.com/download/webinar/2015/MarkMonitor-Webinar-150715-DeepWebDarknetBitcoin.pdf

CONPES. (2011). *Lineamientos de política para Ciberseguridad y ciberdefensa.* [CONPES 3701]. Recuperado de https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3701.pdf

Fazio, H. (2001). La globalización como proceso de larga duración. *Reflexión Política, 3*(5). ISSN: 0124-0781

Finklea, K. (2017). *Darkweb. Congressional Research Service.* Recuperado de https://fas.org/sgp/crs/misc/R44101.pdf

Gaitán, A. (2012). *El ciberespacio: un nuevo teatro de batalla para los conflictos armados del siglo XXI.* Bogotá: Escuela Superior de Guerra.

Gallardo, R. (2017). *La deep web.* Recuperado de https://www.researchgate.net/publication/316884616_La_Deep_Web

INCB (International Narcotics Control Board). (2001). *Globalization and new technologies: challenges to drug law enforcement in the twenty-first century.* Recuperado de https://www.incb.org/documents/Publications/AnnualReports/Thematic_chapters/English/AR_2001_E_Chapter_I.pdf

Larochelle, G. (2004). Las paradojas de la globalización. *Revista Internacional de Sociología, 37*, 177-216.

Petcu, C. (2017). *Globalization and drug traffiking.* Recuperado de https://www.researchgate.net/publication/322602714_Globalization_and_Drug_Traffiking

Sui, D., Caverlee, J. & Rudesill, D. (2015). *The deep web and the darknet: A look inside the internet's massive black box.* Washington D.C.: Wilson Center. Recuperado de: https://www.wilsoncenter.org/sites/default/files/stip_dark_web.pdf

UNODC (United Nations Office on Drugs and Crime). (2010). *The globalization of crime: a transnational organized crime threat assessment.* Recuperado de http://www.unodc.org/res/cld/bibliography/the-globalization-of-crime-a-transnational-organized-crime-threat-assessment_html/TOCTA_Report_2010_low_res.pdf