EDITORIAL ESDEG

Revista
Ciberespacio, Tecnología e Innovación
Volumen 2, número 3, enero-junio 2023
Bogotá, D.C, Colombia
ISSN: 2955-0270 • eISSN: 3028-3310
Página web: https://esdegrevistas.edu.co/index.php/rcit

Dark web: Sistema para la desestabilización de la seguridad nacional

Dark web: System for the destabilization of national security

Hugo Rene Aguillon Gómez

CITACIÓN APA:

Aguillon Gómez, H. R. (2023). Dark web: Sistema para la desestabilización de la seguridad nacional. *Ciberespacio, Tecnología e Innovación, 2*(3), 5-24. https://doi.org/10.25062/2955-0270.4774

Publicado en línea: **Junio 30 de 2023**

Enviar un artículo a la Revista

Revista Ciberespacio, Tecnología e Innovación
Volumen 2, número 3, enero-junio 2023 (pp. 5-24)
Bogotá, D.C, Colombia

EDITORIAL ESDEG

Dark web: Sistema para la desestabilización de la seguridad nacional

Dark web: System for the destabilization of national security

DOI: https://doi.org/10.25062/2955-0270.4774

Hugo Rene Aguillon Gómez
Escuela Superior de Guerra "General Rafael Reyes Prieto", Bogotá D. C., Colombia

Resumen

El siguiente artículo tiene como propósito exponer aquellas vulnerabilidades que surgen gracias a la diseminación de nuevos escenarios bélicos en contextos como el cibernético. Para ello, en primer lugar, se hace una descripción con respecto a la finalidad de desestabilización nacional en el contexto cibernético de la Dark Web, seguido de la identificación de las herramientas existentes dentro de la Dark Web que permiten la desestabilización de la seguridad nacional como medio para dicho fin. Finalmente, se expone el escenario ideal que proteja la seguridad nacional ante los efectos y consecuencias del uso de las herramientas de la Dark Web como medio para la desestabilización nacional.

Palabras Clave: seguridad nacional, ciberespacio, amenaza, desestabilización, Dark Web y consolidación.

Abstract

The purpose of the following article is to expose those vulnerabilities that arise thanks to the dissemination of new war scenarios in contexts such as cyber. To do this, firstly, a description is made regarding the purpose of national destabilization in the cybernetic context of the Dark Web, followed by the identification of the existing tools within the Dark Web that allow the destabilization of national security as means to that end. Finally, the ideal scenario that protects national security from the effects and consequences of the use of Dark Web **tools as a means for national destabilization is presented.**

Key words: national security, cyberspace, threat, destabilization, Dark Web, and consolidation.

Artículo de reflexión
Recibido: 25 de marzo de 2023 • **Aceptado:** 1 de mayo de 2023
Contacto: Hugo Rene Aguillon Gómez aguillonh@esdeg.edu.co

Introducción

La guerra, afirma Prandini et al., (2011) que es una disciplina en constante cambio que ha evolucionado junto con la civilización humana durante casi toda la historia registrada. Desde el momento en que los primeros cazadores elaboraron la primera lanza, desde la primera guerra que se produjo entre dos tribus, hasta la dinámica de la guerra moderna del mundo actual, la guerra ha evolucionado en paralelo con la humanidad. A medida que la guerra se expande, también lo hacen los dominios en los que se libra. Se disputa inicialmente por tierra, luego por el mar y luego por el aire; se lanzan satélites al espacio y luego se crean armas antisatélites para destruir esos mismos satélites que se han colocado en el espacio.

En la actualidad, autores como Ortega y Font (2012) expresan que las naciones se enfrentan amenazas de seguridad nacional reales y difíciles; el extremismo, el terrorismo internacional, el narcotráfico, la trata de personas, entre otros. Estos florecen en variadas áreas del mundo, amenazando a componentes como las instituciones fundamentales para el Estado, los aliados internacionales y la soberanía. Generalmente, Galindo (2005) afirma que los conflictos regionales pueden tener efectos graves sobre los intereses de cada una de las naciones, pues los gobiernos extranjeros con la actividad hostil y los grupos u organizaciones armadas profundizan en la adquisición de capacidades y herramientas sin medir el nivel de daño concurrente por su accionar.

Sin embargo, Acosta et al., (2009) indica que aun con la existencia de amenazas comunes y previamente analizadas, las coacciones más recientes a las que se enfrentan los Estados, y quizás las de más rápido crecimiento, son las que concurren en ambientes tales como el ciberespacio. El uso de las Tecnologías de la Información y las Comunicaciones-TIC's se ha generalizado en la vida diaria de la población mundial. Este nuevo escenario de posibilidades, ofrece un desarrollo sin precedentes en el intercambio de información y comunicaciones, pero al mismo tiempo, lleva a graves riesgos y amenazas que pueden afectar a la seguridad nacional. Estas son conocidas como amenazas cibernéticas, las cuales indica Gómez et al., (2014) que aumentan cada año en frecuencia, alcance y gravedad del impacto. Los ciberdelincuentes, los piratas informáticos y los adversarios extranjeros se están volviendo cada día más sofisticados, siendo capaces de utilizar herramientas alternas como la Dark Web con fines de alto impacto y gran alcance.

Esta, afirma Barrio (2017) que es el colectivo oculto de sitios de Internet a los que solo se puede acceder mediante un navegador web especializado. Se utiliza para mantener la actividad de Internet anónima y privada, lo que puede ser útil tanto en aplicaciones legales como ilegales. Si bien, algunos lo usan para evadir la censura de las instituciones de control de los Estados, pero también se sabe que se utiliza para actividades altamente ilegales. Como nación, Atienza y Bermejo (2020) expone que la ciudadanía al adaptarse a

las revoluciones y avances tecnológicos hoy en día depende del Internet, pues es viable y aplicable a los usos más comunes de la vida cotidiana. No obstante, así como el ciberespacio ofrece grandes oportunidades, también presenta vulnerabilidades, y estas se materializan de forma impactante en espacios tales como la Dark Web.

Ante ello, Aguilar (2015) expone que existen varios factores que contribuyen a la proliferación de acciones delictivas en el ciberespacio, y precisamente en espacios como la Dark Web; i) la rentabilidad de explotarlo en términos económicos, políticos o de otro tipo; ii) la facilidad y bajo costo de emplear las herramientas del sistema para organizar ataques; iii) la facilidad con la que los atacantes pueden esconderse y realizar estas actividades de forma anónima y desde cualquier parte del mundo, con impactos transversales en el público y del sector privado y de los propios ciudadanos.

Al sintetizar los delicados y concurrentes malos manejos del internet, Gamón (2017) afirma que sus actores son criminales motivados por el lucro, particularmente en las áreas de robo de identidad y otras formas de ciberdelito financiero. El costo del delito cibernético, que ya asciende a miles de millones de dólares, aumenta cada año. Para el año 2021, el IBM (2021) reporta un aumento del 10% con respecto al 2020, materializado en 1,07 millones de dólares. Pero, las amenazas cibernéticas también provienen de estados nacionales y otros actores que buscan explotar información para obtener una ventaja sobre los otros. En la actualidad, Marín et al., (2019) indica que los grupos terroristas y extremistas utilizan el poder de la Dark Web, para difundir sus mensajes de odio e intolerancia y para reclutar nuevos miembros, a menudo dirigidos a jóvenes vulnerables. Esto, a diferencia de las redes sociales como Twitter, Instagram, Facebook, entre otras, se moviliza bajo un espacio completamente ilegal, permitiendo el no seguimiento de sus actos, lo que la convierte en una herramienta de ato letalidad para la sociedad.

El alcance global del ciberespacio y la complejidad de sus redes brindan a los malos actores amplios lugares para esconderse, a salvo del alcance del derecho internacional. Para hacer frente a estas amenazas, es importante comprender el *modus operandi* de los atores que actúan bajo la protección de herramientas como la Dark Web, estableciendo inicialmente quiénes son, dónde están y cuáles son sus capacidades, planes e intenciones. Por ello, resulta pertinente establecer como punto de partida: ¿Cuáles son los aspectos de la Dark Web que se utilizan para la desestabilización dentro del contexto de la seguridad nacional?

Metodología

Para el desarrollo del siguiente artículo de investigación se utilizará en primer lugar un enfoque cualitativo, dado que es necesario recolectar información de fuentes primarias como análisis de expertos, bases de datos, artículos, libros, entre otros. Esta información,

según Hernández et al (2014) debe encontrarse fundamentada en material científico, académico y previamente aprobado por tanques de pensamiento enfocados en investigación de orden cualitativo. Asimismo, el tipo de investigación a utilizar será netamente exploratorio, situación que transcurre por la necesidad de estudiar una problemática que no se encuentra totalmente definida.

Debido a la complejidad del caso, el paso a paso de la investigación iniciara con una contextualización teórica, legal e histórica con respecto al desarrollo y evolución de la Dark web como amenaza a la seguridad de las naciones, seguido de una comparación que refleje las características, ventajas y desventajas que concurren por medio del uso de la Dark Web para la seguridad nacional. Finalmente, se expondrán las afectaciones que genera el uso de herramientas como la Dark Web, todo enfocado al desarrollo de nuevas amenazas, tipos de guerra y estrategias de orden hibrido que concurren en el orden internacional y su necesidad de poder.

Marco teórico y conceptual

Para el desarrollo del marco teórico, se debe contextualizar teórica y conceptualmente denominaciones como internet, espacio cibernético, amenaza nacional, seguridad y defensa. Estos, están encaminados de acuerdo a las herramientas hibrida para acceder a la Deep Web, pues autores como Rodríguez (2016) indican que su utilización va más allá del acceso a la información y a su poca trazabilidad en detección. No obstante, aun con estas bases teóricas, resulta preciso determinar a los aspectos de desestabilización que concurren de forma constante en el espacio cibernético. Siendo ejemplos ya materializados que han impactado la seguridad y consolidación de las naciones: Dataleaks y Wikileaks.

Dataleaks

Para autores como Parno et al., (2009), una fuga de datos o Dataleaks ocurre cuando los datos confidenciales se exponen accidentalmente de forma física, en Internet o en cualquier otra forma, incluidos discos duros o computadoras portátiles perdidos. Esto, concurre en un riesgo de alto alcance cuando un ciberdelincuente puede obtener acceso no autorizado a los datos confidenciales sin esfuerzo. En esta fuga, Shu et al., (2015) expone que existen dos formas de acceder a la información; la primera, se expone como una violación de datos, la cual es cuando un ataque exitoso puede proteger información confidencial; la segunda es la fuga de datos que no requiere un ataque cibernético, y generalmente, se debe a prácticas deficientes de seguridad de datos o accidentes del manejo humano.

Wikileaks

De acuerdo con Sirfry (2011), Wikileaks es una organización de medios y sitio web que funcionaba como cámara de compensación para información clasificada o privilegiada. Esta fue fundada en 2006 por el programador informático y activista australiano Julian Assange. Este espacio cibernético sostuvo varias acciones legales en su contra, teniendo como ejemplo la publicación de material interno del movimiento de Scientology en 2008, y este grupo amenazó con presentar una demanda por infracción de derechos de autor. WikiLeaks respondió publicando miles de documentos de Scientology.

Internet

El ciberespacio, una rama del desarrollo de la informática y la tecnología digital, en las últimas décadas ha pasado a formar parte y de las estrategias de adaptación, control y monitoreo de los Estados. Esta, afirman Crystal y Tena (2002) que ha sido invaluable para mejorar y agilizar los procesos relacionados con el trabajo, el aprendizaje y el entretenimiento, y afecta virtualmente a todos los campos del quehacer humano. Una vez que Internet se convirtió comercial en 1988, se convirtió rápidamente en un pilar del ciberespacio, ofreciendo acceso económico e inmediato a muchas fuentes de información, trabajo conjunto a larga distancia y más.

Ante ello, someramente se conoce a la internet, según Baluja y Anias (2006) como una red de área amplia global que conecta sistemas informáticos en todo el mundo. Incluye varias líneas de datos de gran ancho de banda que componen la columna vertebral de Internet. Estas líneas están conectadas a los principales centros de Internet que distribuyen datos a otras ubicaciones, como servidores web e ISP. Por otro lado, el internet se manifiesta por medio del espacio cibernético o ciberespacio, que, de acuerdo con Fernández (2016) se refiere al mundo de las computadoras virtuales y, más específicamente, a un medio electrónico que se utiliza para facilitar la comunicación en línea. La característica principal del ciberespacio es un entorno interactivo y virtual para una amplia gama de participantes. Aun al desarrollarse como herramienta que provee beneficios a la humanidad, existen actores que hacen de esto, una materialización de amenaza bastante volátil. Por ello, resultará pertinente resaltar al ámbito de la seguridad y defensa, partiendo del conocimiento de la amenaza y los riesgos que allí suscitan.

Deep web

Ante la proliferación de herramientas beneficiosas y útiles para la sociedad, He et. al, (2007) expresa que la existencia de escenarios profunda y ocultos como la Deep Web va más allá de intereses individuales. De hecho, esta se encuentra debajo de la superficie del ciberespacio y representa aproximadamente el 90% de todos los sitios web (He et. al,

2007). Esta, sería la parte de un iceberg debajo del agua, mucho más grande que la red de la superficie, dado que esta red oculta es tan grande que es imposible descubrir exactamente cuántas páginas o sitios web están activos al mismo tiempo.

Ante ello, Madhavan (2008) expone que los grandes motores de búsqueda podrían considerarse como barcos de pesca que solo pueden «atrapar» sitios web cerca de la superficie. Todo lo demás, desde revistas académicas hasta bases de datos privadas y más contenido ilícito, está fuera de alcance. Esta web profunda también incluye la parte que conocemos como la web oscura.

Web Oscura o Dark Net

Según Madhavan et al (2008) esta se refiere a sitios que no están indexados y solo son accesibles a través de navegadores web especializados. Significativamente más pequeña que la diminuta red superficial, la web oscura se considera parte de la web profunda. Usando el ejemplo imagen del océano y el iceberg, la red oscura sería la punta inferior del iceberg sumergido. Sin embargo, la web oscura es una parte muy oculta de la web profunda con la que pocos interactuarán o incluso verán, requiriendo únicamente redes como Tor[1]. En otras palabras, la web profunda cubre todo lo que hay debajo de la superficie que todavía es accesible con el software adecuado, incluida la web oscura.

Finalidad de desestabilización nacional en el contexto cibernético de la Dark Web

Para autores como Ibáñez (2017), los Estados sostienen día a día acciones de supervivencia ante el contexto internacional. Este escenario promueve un sinnúmero de estrategias, actividades y necesidades acordes a la forma en que se materializan nuevos riesgos y o, amenazas, siendo evaluadas de acuerdo a su presentación, modo y lugar. En efecto, al hacer especial énfasis en espacios como el cibernético, es importante encaminar las ocurrencias presentadas en sistemas como la Dark Web, dado que se presenta como un sistema difícil de estudiar, pero con grandes intervenciones a lo largo de la historia.

Comprender la aplicación de la Dark Web al futuro de la guerra cibernética requiere que se analice el problema desde múltiples perspectivas. Por supuesto, Mariano (2020) enfatiza en la perspectiva de seguridad nacional subyacente que debería impulsar el entendimiento fundamental de la misma. Desde una perspectiva económica, Es necesario considerar que la aplicación principal de la Dark Web, hasta ahora, ha sido como un mercado utilizado por aquellos que desean participar en el comercio ilícito. La capacidad de comprender el comercio ilícito en la Dark Web en su aplicación a la seguridad nacional,

1 The Onion Router; ed que implementa una técnica diseñada con vistas a proteger las comunicaciones.

afirma Hirane (2021) que requiere la consideración de conceptos como la oferta, la demanda, la reputación del proveedor, entre otros. Mientras que, desde la perspectiva de las operaciones de inteligencia, la Dark Web también puede verse como un terreno neutral para dos partes que desean participar de forma anónima en el intercambio de información, armas y secretos de seguridad nacional.

Al igual que la descripción de la era de la Guerra Fría de un agente clandestino que se encuentra con su fuente en un lugar seguro o que se comunica con agentes a través de puntos muertos, la Dark Web en muchos sentidos se puede considerar como el medio cibernético a través del cual dos profesionales de inteligencia pueden reunirse e intercambiar información de forma segura en terrenos neutrales. Ante ello, López (2019) expone que uno de los principales desafíos para los profesionales de seguridad nacional al analizar la Dark Web es la dificultad para llegar a un entendimiento común de lo que implica el término. El término Dark Web ya es ambiguo, y a menudo, autores como Huidobro y Guerrero (2021) expresan que se combina con otros términos como Deep Web o Criminal Underground.

Las agencias de inteligencia de todo el mundo explotan regularmente la inteligencia de fuentes abiertas (OSINT) que se encuentra en la web de ingreso abierto; mientras que la Deep Web es la ubicación elegida por aquellos ciberdelincuentes que desean participar en la compra y venta de datos de identidad robados, como números de seguridad social y otra información de identificación personal. Sin embargo, Garnacho (2018) expresa que la Dark Web es accesible solo a través de un protocolo de navegación de Internet especial, como The Onion Router (TOR). Este, proporciona anonimato al guiar el tráfico de Internet a través de otros nodos o computadoras que usan el navegador. Este tráfico rebota a través de los nodos TOR hasta que finalmente concurre a través de un nodo de salida. Esto expone Riva (2016) que crea una cebolla o un anonimato de varias capas, situación que permite la protección del anonimato por medio del rebote de sus comunicaciones en una red distribuida en retransmisiones administradas por voluntarios en todo el mundo; aquí, se evita que alguien que esté viendo su conexión a Internet sepa qué sitios se visitan, además del imposible rastreo de ubicación física.

Desde una perspectiva de seguridad nacional, la proliferación incontrolada de usuarios en la Dark Web plantea muchas preocupaciones, ya que estas capacidades han demostrado históricamente que están creadas para afectar significativamente el ámbito de la seguridad nacional. Por ejemplo, Ramírez (2020) expone la experiencia vivida con espacios como Stuxnet[2], la cual es una supuesta capacidad de malware estadounidense-israelí diseñada para interrumpir las centrifugadoras de enriquecimiento de uranio

2 Stuxnet es un gusano informático que afecta a equipos con Windows, descubierto en junio de 2010 por VirusBlokAda, una empresa de seguridad ubicada en Bielorrusia. Es el primer gusano conocido que espía y reprograma sistemas industriales, en concreto sistemas SCADA de control y monitorización de procesos, pudiendo afectar a infraestructuras críticas como centrales nucleares. (John, 2010).

iraníes en Natanz, es quizás el ejemplo más conocido de cómo pueden afectar significativamente los intereses de seguridad nacional de los Estados-nación.

Desde el descubrimiento de Stuxnet, Chen y Abu (2011) indican que los ciberdelincuentes, con el deseo de monetizar su capacidad para desarrollar exploits de tecnología de la información, han aprovechado en gran medida los mercados de la Dark Web para encontrar posibles compradores para sus capacidades. El anonimato facilitado por la Dark Web la convierte en una salida accesible y segura para encontrar exploits antes de su anuncio público, lo que permite a los atacantes comprar estos exploits y lanzarlos antes de que se publiquen los puntos de vulnerabilidad.

El anonimato facilitado a través de la Dark Web fomenta un terreno comercial ideal para los posibles compradores y vendedores de armas peligrosas. Esto, afirma Farwell (2011) que más que teórico, es un hecho que ha sido probado a través de la observación una y otra vez. El Uranio, uno de los compuestos químicos más peligrosos para la composición de armas de fuego es una de la muestra de los tipos de armas que se han incluido en la Dark Web. En respuesta a ello, Fidler (2011) indica que la comunidad global de aplicación de la ley ha estado persiguiendo agresivamente a los compradores y vendedores de armas en la Dark Web, y en muchos casos, han tenido éxito en frustrar posibles ataques. En 2016, Chertoff (2017) afirma que la Oficina Federal de Investigaciones-FBI colaboró con las autoridades policiales irlandesas para evitar que un militante del Ejército de la República de Irlanda (IRA) adquiriera pistolas, granadas y explosivos plásticos de un mercado de la Dark Web. No obstante, mientras la comunidad de seguridad nacional puede reclamar victorias menores con este tipo de operaciones preventivas, los interesados en comprar y vender armas cinéticas de forma anónima han comenzado a cambiar su metodología.

Ante ello, autores como Baravalle et al., (2016) afirman que, es necesario evaluar las dos grandes evoluciones en las que se comercializan las armas cinéticas en la Dark Web. La primera, es que los compradores y vendedores de armas de la Dark Web probablemente trasladen su negocio de algunos de los mercados de acceso abierto más populares a otros mercados que requieren un mayor grado de investigación para ingresar; esto, argumenta la tendencia de materialización por dos puntos principales. El primero es que las personas que se dedican al comercio de armas se están volviendo más cautelosas ante la presencia encubierta de las fuerzas del orden y la posibilidad de que las atraigan a una trampa. La segunda, es que es probable que los principales mercados se estén volviendo menos tolerantes con el riesgo en el que incurren al permitir la inclusión de armas en sus mercados.

Históricamente, Chertoff (2017) indica que las listas de armas han atraído la atención de la comunidad policial mundial, lo que ha provocado que agentes encubiertos examinen los mercados en busca de pistas. Más allá del aumento del riesgo, el margen

de beneficio del mercado para el comercio de armas es relativamente bajo en comparación con los márgenes de beneficio de otros bienes ilícitos de gran volumen, como las drogas y el fraude.

Herramientas de desestabilización existentes dentro de la Dark Web: afectación a la seguridad nacional

Para autores como Biddle et al., (2002), la Darknet se ha convertido, en los últimos años, en uno de los temas más discutidos en los círculos de ciberseguridad. Para algunos, las redes ocultas en Internet son un medio para alcanzar la libertad; mientras que, para otros, estas redes no son más que nuevas salidas para expresar sus deseos criminógenos. En general, la Darknet tiende a ser representada por varios medios de comunicación como un entorno en el que las actividades delictivas surgen de forma natural, incluso hasta el punto de ser un acto fuera de la legalidad.

El tener acceso a la Dark Web y encontrar sitios ocultos es relativamente fácil Moore y Rid (2016) indica que, la parte más desafiante del trabajo es reducir su búsqueda para encontrar inteligencia de amenazas significativas y procesables. No obstante, cuando se enfatiza en centralizar las herramientas que actúan a favor de la Darknet, estas, materializan un sinnúmero de riesgos que desestabilizan el orden de las naciones. Bailey et al., (2006), expone que los riesgos macro de este entorno cibernético se encuentran en la aplicación y uso de tres herramientas principales: i) vulnerabilidades y exploits; ii) portales de acceso; y iii) uso indiscriminado de contraseñas. Estas herramientas, concebidas como debilidades para las estrategias de protección de un Estado, son precisamente capacidades usadas para contrarrestar delitos cibernéticos.

Al hacer una evaluación precisa de estas herramientas, Fachkha y Debbabi (2015) indica que las vulnerabilidades y exploits son la puerta inicial para ataques y delitos nacionales desde la Darknet. Es claro que todos los medios cibernéticos tienen vulnerabilidades, y esto ha generado que cada vez más proveedores e investigadores de seguridad crean vulnerabilidades de software para proteger a los usuarios de los riesgos resultantes.

Lamentablemente, Wood (2009) afirma que los ciberdelincuentes a veces se adelantan a los proveedores y a las comunidades de seguridad; este adelanto es transferido a los tres niveles de toma de decisiones, sin importar si en el nivel estratégico se invierte en herramientas de alto valor financiero y alta capacidad de protección, dando por sentado que ni las organizaciones ni los Estados logran resguardarse en su totalidad a los daños cibernéticos.

Ante ello, autores como Nunes et al., (2016) expresan que por medio de la Darkweb es posible implementar las vulnerabilidades de día u hora cero; estas, son fallas de

seguridad que aún no son conocidas por el proveedor, además de ser vulnerabilidades a las que aún no se les ha encontrado un método de neutralización. Encontrar información sobre las vulnerabilidades de día cero y los exploits que los piratas informáticos discuten y comercian en los mercados oscuros, permite a los profesionales de seguridad identificar e implementar controles de mitigación temporalmente efectivos, dado que su trascendencia e innovación dependen del progreso y nivel de desarrollo tecnológico y científico.

Además de las vulnerabilidades y los exploits, Broséus (2017) indica que los ciber-delicuentes suelen vender acceso activo a sistemas y dispositivos en los mercados oscuros. Muchos de estos delincuentes se especializan en una fase específica del proceso de piratería, pues aquellos que se destaquen en escanear y obtener acceso a las redes deciden no explotar el objetivo ellos mismos. Estos, indica McCormick (2013) que venden el acceso a otros piratas informáticos que se especializan en una mayor exploración y explotación, generando una cadena interminable de vendedores de datos que se han recopilado a atacantes centrados en la extorsión.

Por otro lado, el uso indiscriminado a contraseñas es expuesto por Benjamín et al., (2019) como una mercancía oscura popular. Las contraseñas, son elementos valiosos para los atacantes cibernéticos, dado que conocen el mal hábito de las personas con respecto a reutilizar sus contraseñas en varias cuentas. Esta herramienta perjudicial de la Darknet busca detectar a aquel personal con información privilegiada de las organizaciones, pues Choi et al., (2014) expresa que los proveedores que buscan vender credenciales, propiedad intelectual o datos corporativos importantes en los mercados oscuros generan ingresos de cantidades significativas.

Cualquier tipo de delito con acciones encubiertas, ya sea que involucre drogas, dinero o incluso seres humanos, puede cometerse en la Dark Web. Los rincones más oscuros de Internet son simplemente una plataforma para innumerables delitos. Si se enlistan estas acciones en contra del estado y de la ciudadanía, McCormick (2013) hace especial énfasis a acciones como el asesinato por contrato, el chantaje o la extorsión, venta de drogas ilegales, ventas ilegales de armas, tráfico sexual, terrorismo, pornografía infantil, entre otros. Cuando la tasa de criminalidad en un Estado crece, se generan amenazas, riesgos y dificultades para la consolidación del territorio. Independientemente del medio o forma en que estos se materialicen, al impactar los principios, prioridades y tareas inherentes de los ciudadanos, concurre entonces en un daño a la seguridad y defensa nacional, la cual, en teoría, es una de las obligaciones primordiales de los niveles estratégicos nacionales.

Si se enfatiza en los cuatro campos del poder de los Estados, Cambiaso et al., (2019) indica que uno de los campos con mayor intervención es el social. En efecto, Wood (2009)

afirma que la Darknet se utiliza para una amplia gama de actividades sociales. Estas, van desde ser claramente aceptables desde el punto de vista moral, hasta ser consideradas como ilícitas por algunas personas, o ser visiblemente delictivas según los marcos legislativos nacionales y/o internacionales. Estas actividades, expone Cohen et al., (2020) que podrían agruparse en tres principales: i) activismo, periodismo y denuncia de irregularidades; ii) actividades delictivas en mercados virtuales; y iii) amenazas a la seguridad cibernética que incluyen botnets, malware y secuestro de datos.

Como cualquier tecnología, Miró (2012) expone que el anonimato se puede utilizar tanto para bien como para mal. Usuarios que temen por represalias económicas o políticas por sus acciones usan la web oscura para su protección. Pero también, están aquellos que aprovechan este anonimato en línea para utilizar el Dark Web para actividades ilegales como sustancias ilegales, comercio, transacciones financieras ilegales, robo de identidad, entre otros. Aquí, Rayón y Gómez (2014) indica que el crimen virtual no es diferente al crimen en el mundo real, simplemente se ejecuta en un nuevo medio; es básicamente lo mismo que el crimen terrestre. Sin duda, algunas de las manifestaciones son nuevas, pero una gran cantidad de delitos cometidos con o contra computadoras difiere solo en términos del medio. Mientras que la tecnología de implementación, y particularmente su eficiencia, puede ser sin precedentes, el crimen es fundamentalmente familiar. Este se trata de un fenómeno que hace uso de nuevas herramientas.

Generalmente, las herramientas que atacan la estabilidad de los Estados, aun al estar relacionadas con otros niveles de toma de decisión, Sánchez (2012) afirma que no hay nada único o nuevo en gran parte del ciberdelito: acoso, fraude, propaganda ilegal, pornografía, hurto, blanqueo de capitales, espionaje, etc., excepto el uso del ciberespacio. Pero hay otro nivel de delincuencia que no podría existir sin el ciberespacio: spam, fraude de clics, varios tipos de malware, redes de computadoras cautivas (botnets), robo de identidad, camuflaje y cifrado de datos y comunicaciones, infracciones informatizadas de instalaciones seguras de gran valor, y automáticas, espionaje a largo plazo en organizaciones seguras, entre otros.

Los ciberdelincuentes, indica Brenner (2012) que están explotando el valor creciente de los datos digitales en todas sus formas, y las formas legales y judiciales en las que diferentes países manejan el ciberespacio. Por su parte, Camacho (2020) expone que el crimen siempre ha sido un fenómeno social generalizado, pues las explicaciones criminológicas combinan la motivación, la oportunidad y la existencia de un factor de protección. Aquí, Temperedi y Marcelo (2015) afirma que dos fuentes diferentes de motivación humana pueden ser identificadas. Muchos motivos del comportamiento delictivo son intrínsecos y no se determinan mediante un análisis de costo-beneficio. No hay razón para creer que un mayor uso de una tecnología u otra cambiaría a los seres humanos su

comportamiento. Por tanto, no es sorprendente que las personas también utilicen el ciberespacio para darse cuenta de sus necesidades y perseguir sus objetivos en actividades legítimas: estudiar, entretenimiento, educación, trabajo, así como en las actividades humanas ancestrales de la guerra y el crimen.

Aunque las naciones desarrolladas han instituido la aplicación de la ley regulada ante los ciberdelitos, sus amenazas y consecuencias, las respuestas estatales no han seguido el ritmo de cambios tecnológicos en el ciberespacio. Un buen ejemplo es expuesto por Piccirilli (2016) como el tradicional atraco a un banco en comparación con el robo cibernético, entendiendo que no es lo mismo desarrollar un seguimiento en el ciberespacio bajo una ruta común como el internet que, bajo la ruta permitida por la Dark Web. El uso de la Dark Web expone efectivamente las debilidades de las instituciones de control y monitoreo de los Estados, desestabilizando factores como la institucionalidad, la misionalidad, la integridad, entre otros.

En una seguridad tradicional de robo a un banco, los arreglos deben ser moderados como la posibilidad de un enfrentamiento con armados, dado que es probable que haya guardias. Incluso si el robo en sí tiene éxito, las autoridades logran perseguir a los ladrones en los años venideros. A medida que se ha desarrollado el ciberespacio, la explotación de su vulnerabilidad también ha llegado a abarcar el robo de bancos. Por otro lado, otro ejemplo es indicado por Ballesteros y Hernández (2014), cuando el uso de redes de bots[3] que comprenden decenas de miles de computadoras para el robo extendido de datos de identificación a sitios bancarios, luego se utilizan para robar pequeñas cantidades de dinero, es bastante común.

Dado el problema de atribución en el ciberespacio, las posibilidades de identificar los delincuentes y protagonistas son escasos. Arango (2017) indica que todas las organizaciones que manejan información de alto valor, entre ellas las naciones, son muy conscientes del riesgo de sus intereses y, junto con los organismos reguladores, están tomando pasos para protegerse, invirtiendo en seguridad tecnológica para minimizar el alcance de oportunidad disponible para los ciber delincuentes. Aun así, lo inmediato del riesgo físico sigue siendo sustancialmente menor para el delincuente cibernético que para el delincuente tradicional. El riesgo de castigo legal también es menor, ya que el sistema judicial generalmente percibe el fraude cibernético como un delito de cuello blanco y tratado en consecuencia.

3 Es un programa informático que efectúa automáticamente tareas reiterativas mediante Internet a través de una cadena de comandos o funciones autónomas previas para asignar un rol establecido.

Escenario de ciberseguridad vinculado a los efectos y consecuencias del uso de las herramientas de la Dark Web como medio para la desestabilización nacional.

Para autores como Gayozzo (2021), los escenarios bélicos actuales se encuentran compuestos por una gran cantidad de factores ajenos a los actos y costumbres de guerra cotidiana. De hecho, estos escenarios se encuentran amarrados y adaptados a cualquier forma de guerra, la cual, aun con estar limitada y monitoreada legalmente, ha tenido grandes mutaciones derivadas del desarrollo tecnológico, científico y militar de los Estados. Hoy por hoy, Gil (2019) expone que, entre estos escenarios, existe la necesidad de proponer y/o identificar las estrategias de protección y contención hacia ambientes como el ciberespacio, precisamente aquellos que prosperan en contextos como la Dark Web. El ciberespacio indica Leal (2016) que es un componente integral de todas las facetas de la sociedad, incluida la economía y la defensa. Sin embargo, las entidades públicas y privadas aún luchan por proteger sus sistemas, y los adversarios han aumentado la frecuencia y la sofisticación de sus actividades cibernéticas maliciosas. Una de estas amenazas es conocida como *Ramsomware*, expuesta por XXX como aquel un tipo de software malicioso que impide o limita que los usuarios accedan a su sistema, ya sea bloqueando la pantalla del sistema o bloqueando los archivos de los usuarios hasta que se pague un rescate.

Esto, afirma San Martín (2019) que ha llevado a un mayor interés en otros temas, además de los militares tradicionales, dado que las amenazas contra los Estados, en particular el poder blando y otros medios de influencia no militar, han permeado las actividades cotidianas de la ciudadanía; Colombia, no es una excepción a ello. En la definición original, Fernández-Sánchez (2016) indica que el poder blando es similar al poder de atracción, pero, la reinterpretación del mismo también implica la posibilidad de ejercer un poder blando contra otros actores, con el fin de ganar influencia o participar en una guerra no militar.

Ante estas circunstancias, naciones como Colombia, expuestas a amenazas tanto internas como externas, debe buscar la aplicación de estrategias ante escenarios como el cibernético, dado que atacan la seguridad de una manera silenciosa pero incisiva. Badrán y Niño (2020) exponen que la prosperidad y la seguridad de Colombia dependen de cómo responder a las oportunidades y desafíos en el ciberespacio, en la infraestructura crítica, en la defensa nacional y en la vida diaria de los colombianos. Generalmente, un espacio competente para soportar cualquier intento de daño o intervención se basa en tecnologías de la información interconectadas e impulsadas por computadoras, precisamente alineadas a la vanguardia tecnológica del momento. Aquí, gracias a que todas las facetas de la vida se han vuelto más dependientes a un ciberespacio seguro, se han revelado nuevas vulnerabilidades y nuevas amenazas.

El auge del internet y la creciente centralidad del ciberespacio a todas las facetas del mundo moderno corresponden al ascenso de las naciones en dinámicas como la globalización. Llinares (2011) afirma que al menos por el pasado cuarto de siglo, la gente impulsó la evolución del ciberespacio, y a su vez, este logró consolidarse como fundamental para la creación e innovación de riqueza en los Estados. Por ello, el ciberespacio es un componente inseparable de los servicios financieros, sociales, gubernamentales y políticos. No obstante, al menos en Colombia, existen adversarios que han adoptado un enfoque opuesto, pues se benefician del Internet abierto. Estos, generalmente, se esconden detrás de las nociones de soberanía mientras imprudentemente violan las leyes al participar en espionaje pernicioso, económico y malicioso, además de sostener actividades cibernéticas que provocan importantes interrupciones y daño a personas. Estos, indica Zarate (2014) que ven el ciberespacio como una arena donde el poder militar, económico y político podría ser neutralizado, siendo entonces Colombia una nación altamente vulnerable.

En este contexto, las nuevas amenazas y una nueva era de competencia estratégica exigen una nueva estrategia cibernética que responda a realidades, reduzca vulnerabilidades, disuada adversarios y salvaguarde las oportunidades para que el pueblo colombiano prospere. Asegurar el ciberespacio es fundamental para la estrategia nacional y requiere avances técnicos y administrativos de gran eficiencia en todo el Gobierno Nacional. Ambos (2015), indica que también se debe reconocer que un enfoque puramente tecnocrático al ciberespacio es insuficiente para abordar la naturaleza de los nuevos problemas que se enfrentan.

Como ejemplo a ello, Sohr (2018) expone que los Estados participan en una competencia continua contra adversarios estratégicos, estados rebeldes y redes terroristas y criminales. Al hacer mención de actores como Estados Unidos, Aguilar (2021) indica que Rusia, China, Irán y Corea del Norte utilizan al ciberespacio como un medio para desafiar a los Estados Unidos, a sus aliados, y a sus socios, siendo a menudo una imprudencia que no fue considerada en otros dominios. Estos utilizan herramientas cibernéticas para socavar la economía y democracia norteamericana, entendiendo que entre estos Estados existe una carrera de dominio y control del orden internacional.

Ante el orden y la necesidad que concurre para proteger el Estado y las actividades de la nación colombiana, Recalde (2021) expresa que es necesario implantar o reforzar la actual estrategia cibernética. Esta, debe contener prioridades como: i) defender la patria protegiendo las redes, sistemas, funciones y datos; ii) promover la prosperidad mediante el fomento de una economía digital y próspera, fomentando la innovación e investigación nacional; iii) preservar la paz y seguridad fortaleciendo la capacidad colombiana, en concierto con aliados y socios, para disuadir y si es necesario castigar a quienes utilicen herramientas cibernéticas con fines maliciosos; y iv) expandir la influencia colombiana

en el extranjero para extender los principios claves de un ciberespacio abierto, interoperable, confiable y seguro.

Por ello, el éxito de la estrategia colombiana podría hacerse realidad cuando las vulnerabilidades de la ciberseguridad sean efectivamente gestionadas mediante la identificación y protección de redes, sistemas, funciones y datos, así como la detección de las mismas en cuestiones perjudiciales, desestabilizadoras, maliciosas y negativas. La articulación de escenarios acordes a combatir herramientas como la Dark Web debe estar organizada según los pilares de la Política de Defensa y Seguridad Nacional de Colombia, haciendo valer los lineamientos de ciberseguridad y ciberdefensa inscritos en el CONPES 3701 con respecto al control, monitoreo y/o neutralización de las amenazas informáticas que atacan significativamente al Estado colombiano.

La responsabilidad de asegurar la infraestructura crítica de la nación y su gestión en escenarios como el que concurre en el ciberespacio es compartido por el sector privado y gubernamental, situación establecida de forma clara durante el Plan Sectorial de Protección y Defensa para la Infraestructura Crítica Cibernética de Colombia (2018). En asociación con el sector privado, es posible utilizar de forma colectiva una gestión de riesgos enfocada para mitigar las vulnerabilidades y aumentar el nivel básico de ciberseguridad en toda la infraestructura crítica. Simultáneamente, Cujabante et al., (2020) afirma que instituciones como las Fuerzas Militares de Colombia- FFMM han venido implantando un enfoque basado en consecuencias para priorizar las acciones, entendiendo que estas estrategias podrían reducir el potencial de adversarios expertos, quienes precisamente podrían causar interrupciones a gran escala o de larga duración en la infraestructura crítica.

Asimismo, la nación tendría que buscar la forma de disuadir a los ciber actores malintencionados, imponiendo para ellos y para sus patrocinadores una variedad de herramientas, que incluyen, pero no se limitan, a enjuiciamientos y sanciones económicas, como parte de una estrategia de disuasión más amplia. Esto, por ejemplo, se encuentra fundamentado bajo esfuerzos multilaterales de organizaciones como la OTAN y la UE, estableciendo leyes en el contexto de la ciberdefensa como el *Tallinn Manual on the International Law Applicable to Cyber Operations*, buscando establecer políticas comunes de acuerdo con la importancia estratégica y operativa en materia de ciberseguridad y ciberdefensa.

Por su parte, González (2016) sugiere que la administración nacional antes de enfocarse en establecer un escenario próspero y propicio para el desarrollo de la nación, debe aclarar los roles y responsabilidades de los organismos e instituciones de control que se encuentren dirigidas a la ciberseguridad, gestión de riesgos y respuesta a incidentes. Esta claridad permitirá una gestión proactiva de riesgos que abordaría de manera integral las amenazas, vulnerabilidades y consecuencias.

Conclusiones

Este artículo de investigación permitió conocer de forma académica cuál es la finalidad de desestabilización nacional en el contexto cibernético de la Dark Web, además de mencionar aquellas herramientas que promueven los daños y la afectación a la seguridad nacional. Tanto la finalidad como las herramientas que actúan paralelamente con la Dark Web, deben ser consideradas como componentes que se desarrollan bajo escenarios cibernéticos de difícil seguimiento y fácil mimetismo, los cuales, en teoría, debilitan los esfuerzos de monitoreo, control y rastreo creados por instituciones como las Fuerzas Militares-FFMM y la Policía Nacional. Aquí, es necesario alertar a las estrategias tanto gubernamentales como operativas sobre la necesidad de intrusión, formación y/o reforzamiento tanto del recurso humano como de la infraestructura critica delegada para las actividades de ciberseguridad y ciberdefensa de la nación, pues componentes como el tecnológico y científico son básicamente catalizadores tanto de protección como de exposición ante este tipo de amenazas.

Asimismo, la nación colombiana está constantemente tratando de presentar nuevas aplicaciones y tecnologías que mejoren las viejas formas de proteger el ciberespacio, ofreciendo nuevas funciones útiles. Pero, la atención a la ciberseguridad puede ralentizar la introducción de nuevos productos y servicios en el mercado, tanto legal como ilegal, con el resultado de que las nuevas tecnologías y aplicaciones a menudo se ofrecen para uso general sin el beneficio de una revisión para una ciberseguridad eficaz. La cuestión de la actividad gubernamental es cómo gestionar el equilibrio entre el ritmo de la innovación y una postura de ciberseguridad más sólida, sin generar entradas a entornos de alto impacto como la Dark Web, entendiendo que su existencia hoy en día ha generado grandes debilidades para la estabilidad de los Estados.

Por otro lado, aun con tener capacidades en infraestructura cibernética significativas, es necesario promover en Colombia una infraestructura cibernética acorde con la evolución tecnológica mundial, la cual cuente con una capacidad de comunicaciones y conectividad interoperable, confiable y segura. Esto proporcionará mayores oportunidades para todos los sectores nacionales. Esto permitirá proteger la nación y los intereses mediante el fortalecimiento de la posición competitiva de la industria en el mundo digital, apoyando y promoviendo prácticas legales en el uso del espacio cibernético, lideradas por la industria y basadas en principios tecnológicos sólidos.

Finalmente, la competencia técnica y la conciencia se consideran cuestiones urgentes para lograr efectivas estrategias en torno a la ciberseguridad en naciones tales como Colombia. Gran parte de este conocimiento es tácito y su relación con la ciberseguridad es directa. Ante ello, existen aspectos por los cuales la nación y su estrategia de control, monitoreo y neutralización de amenazas dependen de forma explícita; la primera, la limitación de recursos es evidente, pero la limitación también influye en

la forma de la estrategia; y la segunda, el progreso y no contención de herramientas de desestabilización como la Dark Web, provee en su mayoría grandes habilidades poco rastreables y detectables, siendo entonces una alerta y alarma para los entes de control gubernamental atentos a eliminar y neutralizar cualquier acción que desestabilice el Estado colombiano.

Declaración de divulgación

Los autores declaran que no existe ningún potencial conflicto de interés relacionado con el artículo.

Autor

Hugo Rene Aguillon Gómez. Magister en Escuela Superior de Guerra General "Rafael Reyes Prieto", Colombia.

Orcid: https://orcid.org/0000-0002-1174-3585 Contacto: aguillonh@esdeg.edu.co

Referencias

Acosta, P., Rodríguez, P., Arnáiz de la Torre, D., & Taboso Ballesteros, P. (2009). *Seguridad nacional y ciber-defensa*. Centro Superior de Estudios de la Defensa Nacional. Catálogo General de Publicaciones Oficiales http://publicacionesoficiales.boe.es/

Aguilar Cárceles, M. M. (2015). Cibercrimen y cibervictimización en Europa: instituciones involucradas en la prevención del ciberdelito en el Reino Unido. *Revista criminalidad*, 57(1), 121-135.

Aguilar, J. S. (2021). *Omnium contra omnes: Análisis político-militar de la guerra en el ciberespacio.* Nau Llibres.

Ambos, K. (2015). *Responsabilidad penal internacional en el ciberespacio.* Universidad Externado.

Arango, R. A. P. (2017). Afectación del cibercrimen en las pymes. La corrupción en la contratación administrativa: el caso de Costa Rica, 8-59 [Conferencia]. 2° Congreso Internacional Crimen económico y fraude financiero y contable

Atienza, G. M., & Bermejo, D. F. (2020). *Ciberdelitos*. Ediciones Experiencia.

Badrán, F., & Niño, C. (2020). Seguridad nacional de Colombia: aproximación crítica a los contrasentidos misionales. *Pensamiento propio*, 51, 103-118.

Bailey, M., Cooke, E., Jahanian, F., Myrick, A., & Sinha, S. (2006, March). *Practical darknet measurement. In 2006 40th Annual Conference on Information Sciences and Systems* (pp. 1496-1501). Institute of Electrical and Electronics Engineers.

Ballesteros, M. C. R., & Hernández, J. A. G. (2014). Cibercrimen: particularidades en su investigación y enjuiciamiento. *Anuario Jurídico y Económico Escurialense*, (47), 209-234.

Baluja-García, Walter, & Anías-Calderón, Caridad (2006). Amenazas y defensas de seguridad en las redes de próxima generación. *Ingeniería y Competitividad*, 8(2),7-16. https://www.redalyc.org/articulo.oa?id=2913/291323467001

Baravalle, A., Lopez, M. S., & Lee, S. W. (2016, December). *Mining the dark web: Drugs and fake IDs. In 2016 IEEE 16th International Conference on Data Mining Workshops* (ICDMW) (pp. 350-356). Institute of Electrical and Electronics Engineers.

Barrio Andrés, M. (2017). *Ciberdelitos: amenazas criminales del ciberespacio*. Editorial Aranzadi.

Benjamín, V., Valacich, J. S., & Chen, H. (2019). DICE-E: A Framework for Conducting Darknet Identification, Collection, Evaluation with Ethics. *MIS Quarterly*, 43(1).

Biddle, P., England, P., Peinado, M., & Willman, B. (2002, November). *The darknet and the future of content protection. In ACM Workshop on Digital Rights Management* (pp. 155-176). Springer

Brenner, S. (2012). La Convención sobre Cibercrimen del Consejo de Europa. *Revista Chilena de Derecho y Tecnología*, 1(1).

Broséus, J., Rhumorbarbe, D., Morelato, M., Staehli, L., & Rossy, Q. (2017). A geographical analysis of trafficking on a popular darknet market. *Forensic science international*, 277, 88-102.

Camacho, D. (2020). AIDACyber: contribuciones en ciberseguridad y cibercrimen. *Information Fusion*, 63, 1-33.

Cambiaso, E., Vaccari, I., Patti, L., & Aiello, M. (2019, February). *Darknet Security: A Categorization of Attacks to the Tor Network*. In ITASEC.

Chen, T. M., & Abu-Nimeh, S. (2011). Lessons from stuxnet. *Computer, 44*(4), 91-93.

Chertoff, M. (2017). A public policy perspective of the Dark Web. *Journal of Cyber Policy, 2*(1), 26-38.

Choi, S. S., Song, J., Kim, S., & Kim, S. (2014). A model of analyzing cyber threats trend and tracing potential attackers based on darknet traffic. *Security and Communication Networks, 7*(10), 1612-1621.

Cohen, D., Mirsky, Y., Kamp, M., Martin, T., Elovici, Y., Puzis, R., & Shabtai, A. (2020, September). DANTE: A framework for mining and monitoring darknet traffic. In *European Symposium on Research in Computer Security* (pp. 88-109). Springer, Cham.

Crystal, D., & Tena, P. (2002). *El lenguaje e Internet* (p. 304). Cambridge university press.

Cujabante Villamil, X. A., Bahamón Jara, M. L., Prieto Venegas, J. C., & Quiroga Aguilar, J. A. (2020). Ciberseguridad y ciberdefensa en Colombia: un posible modelo a seguir en las relaciones cívico-militares. *Revista Científica General José María Córdova, 18*(30), 357- 377. http://dx.doi.org/10.21830/19006586.588

Fachkha, C., & Debbabi, M. (2015). Darknet as a source of cyber intelligence: Survey, taxonomy, and characterization. *Communications Surveys & Tutorials, 18*(2), 1197-1227.

Farwell, J. P., & Rohozinski, R. (2011). Stuxnet and the future of cyber war. *Survival, 53*(1), 23-40.

Fernández, H. M. M. (2016). As novas guerras: O desafio da guerra híbrida. *Revista de Ciencias Militares*, 4.

Fernández-Sánchez, Pablo Antonio (2016). Introducción: Riesgos y amenazas para la seguridad humana. Araucaria. *Revista Iberoamericana de Filosofía, Política y Humanidades, 18*(36),211-215. https://www.redalyc.org/articulo.oa?id=282/28248171010.

Fidler, D. P. (2011). Was stuxnet an act of war? decoding a cyberattack. *Security & Privacy, 9*(4), 56-59.

Galindo Hernández, C. (2005). De la Seguridad Nacional a la Seguridad Democrática: nuevos problemas, viejos esquemas. *Estudios Socio-Jurídicos*, 7, 496.

Gamón, V. P. (2017). Internet, la nueva era del delito: ciberdelito, ciberterrorismo, legislación y ciberseguridad. *URVIO: Revista Latinoamericana de Estudios de Seguridad*, (20), 80-93.

Gayozzo, P. I. E. R. O. (2021). Guerra de quinta generación en la Cuarta Revolución Industrial. *Futuro Hoy, 2*(1), 31-34.

Gómez, F., Vélez, F., Esteso, F., Pascual, D., Pita, R., García, J., & De la Corte Ibáñez, L. (2014). *Seguridad nacional, amenazas y respuestas*. Editorial Almuzara.

González, C. L. (2016). Ciberespacio: un nuevo dominio, un nuevo reto...(I). *Armas y Cuerpos*, (133), 57-64.

He, B., Patel, M., Zhang, Z., & Chang, K. C. C. (2007). Accessing the deep web. *Communications of the ACM, 50*(5), 94-101.

Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, P. (2014). *Metodología de la Investigación* (6ta. ed.). (S. d. Interamericana Editores, Ed.). Mc Graw Hill

Hirane, C. S. (2021). Estrategia Nacional Contra la Delincuencia Organizada Transnacional (DOT) en países Latinoamericanos: ¿desafío de política pública pendiente?. *Análisis del Real Instituto Elcano* (ARI), (20), 1.

Huidobro, C. B., & Guerrero, S. R. (2021). *Amenazados: Seguridad e inseguridad en la web.* Ediciones UM.

Ibáñez, E. M. (2017). *Dark web y deep web como fuentes de ciberinteligencia utilizando minería de datos*. 3ª ÉPOCA, 74.

Leal, P. C. (2016). A guerra híbrida. *Doutrina Militar Terrestre em Revista, 4*(9), 6-17.

Llinares, F. M. (2011). La oportunidad criminal en el ciberespacio. *Revista Electrónica de Ciencia Penal y Criminología*, 7, 1-07.

López Flores, E. D. (2019). *El delito de narcotráfico en la Deep Web: Una visión desde la Legislación Ecuatoriana* [Bachelor›s tesis]. Universidad San Francisco de Quito.

Madhavan, J., Ko, D., Kot, Ł., Ganapathy, V., Rasmussen, A., & Halevy, A. (2008). Google›s deep web crawl. *Proceedings of the VLDB Endowment,* 1(2), 1241-1252.

Mariano Díaz, R. (2020). *La ciberseguridad en tiempos del COVID-19 y el tránsito hacia una ciberinmunidad.* Comisión Económica para América Latina y el Caribe.

Marín, J., Nieto, Y., Huertas, F., & Montenegro, C. (2019). Modelo Ontológico de los Ciberdelitos: Caso de estudio Colombia. *Revista Ibérica de Sistemas e Tecnologías de Informação,* (E17), 244-257.

McCormick, T. (2013). The Darknet. *Foreign Policy,* (203), 22.

Miguel-Gil, J. (2019). El tratamiento informativo de la guerra híbrida de Rusia. *URVIO Revista Latinoamericana de Estudios de Seguridad,* (25), 108-121.

Miró Llinares, F. (2012). El cibercrimen: Fenomenología y criminología de la delincuencia en el ciberespacio. *El cibercrimen,* 1-332.

Moore, D., & Rid, T. (2016). Cryptopolitik and the Darknet. *Survival, 58*(1), 7-38.

Nunes, E., Diab, A., Gunn, A., Marin, E., Mishra, V., Paliath, V., & Shakarian, P. (2016, September). *Darknet and deepnet mining for proactive cybersecurity threat intelligence*. In 2016 IEEE Conference on Intelligence and Security Informatics (ISI) (pp. 7-12). IEEE.

Ortega, P., & Font, T. (2012). Seguridad nacional, seguridad multidimensional, seguridad humana. *Papeles de relaciones Ecosociales y Cambio Global*, 119, 161-172.

Parno, B., McCune, J. M., Wendlandt, D., Andersen, D. G., & Perrig, A. (2009, May). *CLAMP. Practical prevention of large-scale data leaks. In 2009 30th IEEE Symposium on Security and Privacy* (pp. 154-169). Institute of Electrical and Electronics Engineers.

Piccirilli, D. (2016). *Protocolos a aplicar en la forensia informática en el marco de las nuevas tecnologías (pericia–forensia y cibercrimen)* [Doctoral dissertation]. Universidad Nacional de La Plata).

Prandini, P., Maggiore, M., & Carozo, E. (2011). *Panorama del ciberdelito en Latinoamérica.* Proyecto Amparo-Registro de Direcciones de Internet para Latinoamérica y el Caribe (LACNIC).

Ramírez Perea, N. (2020). Criminología y las nuevas tecnologías. Universitat Jaume I. Departament de Dret Públic.

Rayón Ballesteros, M. C., & Gómez Hernández, J. A. (2014). Cibercrimen: particularidades en su investigación y enjuiciamiento. *Anuario Jurídico y Económico Escurialense*, (47), 209-234.

Recalde, L. (2021). El ciberespacio: el nuevo teatro de guerra global. *Revista de Ciencias de Seguridad y Defensa,* 1(2), 5.

Riva, R. C. (2016). El nuevo entorno digital de la actividad criminal/a new digital environment for criminal activity. *Boletín de Estudios Económicos*, 71(219), 591.

Rodríguez Prieto, Rafael (2016). ¿Qué seguridad? Riesgos y Amenazas de Internet en la Seguridad Humana. Araucaria. *Revista Iberoamericana de Filosofía, Política y Humanidades,* 18(36),391-415.

San Martín, H. (2019). *La guerra híbrida rusa sobre Occidente*. Page Publishing Inc.

Sánchez Medero, G. (2012). *Cibercrimen, ciberterrorismo y ciberguerra: los nuevos desafíos del s. XXI.* Thumbnail.

Shu, X., Zhang, J., Yao, D. D., & Feng, W. C. (2015). Fast detection of transformed data leaks. *Transactions on Information Forensics and Security, 11*(3), 528-542.

Sifry, M. L. (2011). *WikiLeaks and the Age of Transparency.* OR Books.

Sohr, R. (2018). La guerra por las mentes en el ciberespacio. *Mensaje, 67*(667), 18-21.

Temperini, M. G., & Macedo, M. (2015). *La problemática de los perfiles falsos en Facebook y su relación con el Cibercrimen. In Simposio Argentino de Informática y Derecho* (SID 2015)-JAIIO 44 (Rosario, 2015).

Wood, J. A. (2009). The Darknet: A digital copyright revolution. *Rich. JL & Tech., 16*, 1.

Zárate Luna, P. A. (2014). Guerra por el Ciberespacio [Bachelor‧s tesis]. Universidad Piloto de Colombia).