EL METAVERSO Y LAS NUEVAS AMENAZAS A LA SEGURIDAD DEL ESTADO

Mayo. de COM. Darwin Manolo Paredes [1]
Mayo. de I. Eduardo Burbano Bolaños [2]

Resumen

El artículo presenta una descripción amplia del metaverso y del espacio cibernético, así como de la utilidad que estas tecnologías proporcionan para enfrentar las nuevas amenazas a la seguridad del Estado ecuatoriano, denominadas amenazas híbridas. De igual forma, se realiza un enfoque a los delitos conexos del narcotráfico y cómo el empleo lesivo del espacio cibernético ha permitido afectar a la infraestructura estratégica del Estado. El objetivo de esta investigación es realizar un análisis descriptivo de las tecnologías antes mencionadas, y proporcionar argumentos válidos que muestren que las actividades ilegales en el metaverso y en el espacio cibernético constituyen una amenaza híbrida. Así mismo, plantea la necesidad de promover el desarrollo de un sistema nacional con capacidad de operar en el espacio cibernético; y de esta forma, alcanzar una respuesta efectiva y oportuna del Estado ante estas nuevas amenazas a la seguridad.

Palabras clave: Amenazas híbridas, Metaverso, Realidad Virtual, Seguridad Nacional.

Abstract

The article presents a broad description of the metaverse and cyberspace, as well as the utility that these technologies provide to face the new threats to the security of the Ecuadorian State, called hybrid threats. In the same way, an approach is made to the related crimes of drug trafficking and how the harmful use of cyberspace has allowed to affect the strategic infrastructure of the nation. The objective of this research is to carry out a descriptive analysis of the aforementioned technologies, and provide valid arguments that show that illegal activities in the metaverse and in cyberspace constitute a hybrid threat. Likewise, the need to promote the development of a national system with the capacity to operate in cyberspace is raised; and in this way, achieve an effective and timely response from the State to these new threats to their security.

Keywords: Hybrid threats, Metaverse, Virtual Reality, National Security.

[1] Academia de Guerra del Ejército - Máster en Ciencias de Ingeniería Electrónica por el Instituto Militar de Ingeniería-Brasil dmparedesc@ejercito.mil.ec
[2] Academia de Guerra del Ejército - Segundo Comandante del Grupo Especial de Comandos No9 - eburbanob@ejercito.mil.ec

DOI: https://dx.doi.org/10.24133/RCSD.VOL16.N01.2023.09
Revista Academia de Guerra del Ejército Ecuatoriano, Volumen 16. Núm. 1 abril 2023. pp. 122 - 133

Introducción

Es importante puntualizar que la presente investigación se orienta en el análisis de las amenazas que hoy en día acechan a la seguridad del Ecuador. De manera específica, aquellas amenazas cuyas capacidades de actuar en el ciberespacio afectan a la infraestructura crítica del Estado, y de ciertas instituciones fundamentales para la vida de la nación.

La investigación profundizó el estudio del metaverso, tecnología que, además de todas sus bondades que permiten recrear y avizorar los escenarios del futuro, también se convierte en una plataforma de intercambio de información que está siendo utilizada por grupos ilegales y organizaciones criminales para perpetrar actividades ilícitas que ponen en riesgo la seguridad de la nación.

Otra de las variables de la presente investigación, son las tendencias de la web profunda y la web obscura, cuya característica y capacidad de actuar en el espacio cibernético también está siendo empleada para realizar actividades lícitas como ilícitas, por lo que el Estado debería tomar más atención de dichos estratos tecnológicos.

En ese contexto, se han planteado tres hipótesis de investigación para el presente estudio, las cuales serán expuestas en esta introducción y serán analizadas a mayor detalle en las secciones subsiguientes, para alcanzar conclusiones que serán de utilidad para entender el accionar de las amenazas híbridas y los retos que enfrenta la sociedad actual.

La primera hipótesis planteada, considera que el metaverso es un medio que permite afectar a la infraestructura crítica del Estado, en especial, aquella infraestructura que se sostiene fuertemente en redes informáticas y de telecomunicaciones, y que por su naturaleza está más expuesta a ataques en la web.

La segunda hipótesis hace referencia a que existe una desatención del Estado en el ámbito de administración y regulación del metaverso, debido a que no se generan normativas o leyes al respecto, las cuales son cada vez más necesarias, debido a que estas plataformas están siendo empleadas con mayor frecuencia por parte de la ciudadanía. Y que, sin duda, en el corto y mediano plazo tendrán un crecimiento exponencial en cuanto a los usuarios de la misma.

La tercera hipótesis de esta investigación considera que fomentar el conocimiento y controlar eficientemente el espacio cibernético permitirá mejorar la capacidad de respuesta del Estado ante el accionar de estas amenazas híbridas, disminuyendo la capacidad de las mismas, para afectar la seguridad del Estado.

Es pertinente señalar que, para el desarrollo de esta investigación, se ha empleado un método inductivo-analítico que parte de hechos y acontecimientos históricos, los cuales permiten inducir que la evolución del uso del metaverso y el espacio cibernético tendrá un crecimiento potencial en el futuro mediato, y que el Estado debe actuar de forma proactiva y prospectiva para ejercer un control efectivo sobre las mencionadas tecnologías.

Por tanto, luego de la introducción planteada, la primera sección presenta un estudio detallado de las amenazas a la seguridad que actualmente enfrenta el Ecuador, entre las cuales destacan las amenazas híbridas y el narcotráfico, con sus delitos conexos, ambas enfocadas desde su accionar en el espacio cibernético.

La segunda sección muestra las definiciones, características y capacidades del metaverso, y orienta al análisis de las mismas, desde el enfoque de seguridad para el Estado. Finalmente, se presentan las conclusiones que arroja la presente investigación.

1. LAS AMENZAS A LA SEGURIDAD EN EL ECUADOR

Previo al estudio detallado de las nuevas amenazas a la seguridad del Estado, consideradas por los autores de esta investigación, es pertinente puntualizar ciertas peculiaridades sobre la seguridad nacional, para lo cual se explicará la estructura del sistema de seguridad pública, y también se presentarán las motivaciones que permiten considerar ciertas actividades en el entorno del metaverso y el espacio cibernético como amenazas a la seguridad.

La Constitución de la República y sus documentos derivados expresan taxativamente la responsabilidad que tiene el Estado para neutralizar toda amenaza a la seguridad y desarrollo de la nación; y para el efecto, se han definido las instituciones u órganos ejecutores de la seguridad, los cuales actúan desde cuatro ámbitos específicos, expuestos en la Ley de Seguridad Pública y del Estado, Capítulo III, artículo 11 (Ley de Seguridad Pública y del Estado, 2009, modificada en 2014), los mismos que se explican a continuación.

El primero es el de la defensa de la soberanía e integridad territorial, el cual está bajo responsabilidad del Ministerio de Defensa, del Ministerio de Relaciones Exteriores y de las Fuerzas Armadas, cada uno en sus ámbitos de competencia. Al respecto, las FF.AA. mantienen en su estructura un Comando de Ciberdefensa, desde el cual, empleando sus capacidades de búsqueda, exploración y respuesta, pueden coadyuvar con el objetivo de neutralizar amenazas en esta esfera (Ministerio de Defensa Nacional, 2019).

El segundo ámbito es el orden público, mismo que está bajo responsabilidad del Ministerio de Gobierno Policías y Cultos, y de la Policía Nacional. En este ámbito, la Policía Nacional dispone del Departamento de Investigación de Delitos Cibernéticos, con responsabilidad de prevenir y disminuir los delitos cometidos en esta área, empleando dispositivos electrónicos, computadores o medios de comunicación (Policía Nacional, 2023).

El tercer ámbito es el de la prevención, mismo que recae sobre todas las instituciones estatales, para lo cual, estas deben dar cumplimiento a las normativas y esquemas de seguridad de la información digital, como una política de prevención de ataques cibernéticos y de protección de la información pública que estas administran.

Finalmente, el cuarto ámbito es el de gestión de riesgos, el cual está bajo la responsabilidad de la Secretaría Nacional de Gestión de Riesgos, en cuya estructura organizacional no se considera una entidad encargada de incrementar la capacidad de actuación en el ciberespacio (SNGR, 2023).

Esta organización que presenta el Estado ecuatoriano para garantizar la seguridad integral hoy enfrenta un escenario muy dinámico, con características de una elevada volatilidad que, de un momento a otro, pueden transformar un escenario de pasividad total, a una condición de inseguridad absoluta.

Por otro lado, en lo referente a las capacidades que derivadas del uso del metaverso y el espacio cibernético pueden configurarse como amenazas a la seguridad del Estado, es pertinente señalar que estas actividades conforman escenarios complejos y volátiles, que incluyen el uso indebido de tecnologías como el metaverso y a las actividades cibernéticas, en muchos de los casos vinculadas al narcotráfico y sus delitos conexos.

Esta consideración de amenaza para el Estado se sustenta en la capacidad, motivación e intención que manejan grupos u organizaciones nacionales y transnacionales para ─empleando plataformas tecnológicas─ atacar a la infraestructura del Estado, tal como sucedió en años anteriores cuando instituciones como el Registro Civil, CNT, CTE, Banco del Pichincha, entre otros, fueron atacados y provocaron caos y zozobra en la población.

Así mismo, en determinadas ocasiones se han observado escenarios complejos e inciertos, como los generados a partir de las protestas sociales del 2019 y 2022, las cuales, bajo la bandera de una protesta social, debidamente justificada, permitieron el accionar de grupos ilegales y de organizaciones vinculadas al narcotráfico, como lo afirma el diario France24 (2022), las cuales causaron caos y muertes. Además, la fuente afirma que el narcotráfico también está financiando las actividades criminales en los centros privados de libertad, y así mismo, el accionar en el espacio cibernético fue elevado, como lo señaló (Accessnow, 2023).

Esta incertidumbre compleja y ambigua ha llevado a la necesidad de replantear los fines, modos y medios con los que el Estado debe enfrentar los escenarios actuales, en los que las amenazas se confunden con protestas sociales o con actividades rutinarias en los diferentes sitios web, y se configuran las denominadas amenazas híbridas.

1.1. Las amenazas híbridas

Sobre la base de lo anteriormente expuesto, se evidencia que las amenazas a la seguridad de un Estado han ido mutando. Esta mutación consiste en la transformación vertiginosa de capacidades a partir del desarrollo técnico y científico, de tal manera que su accionar se torna multidimensional (Galán, 2018); y por tanto, pueden poner en riesgo la estructura tecnológica del Estado, como lo menciona (Sales, 2019).

El término híbrido, en el ámbito de la sociología, fue insertado por Zygmunt Bauman (Barreno-Jardi, 2011) quien, al referirse a las sociedades líquidas, mencionaba que la característica de hibridación tiene un gran potencial, capaz de generar cambios significativos en la forma de vida de las sociedades.

Mientras que en el ámbito militar, la hibridación de las amenazas ha tenido cabida con el aparecimiento de conflictos como Israel-Hezbollah o los actos en que la insurgencia chechena enfrenta al ejército ruso (Colom-Piella G., 2012), o también, el ataque a las Torres Gemelas, como lo menciona Bartolomé (2019), o los conflictos no declarados que fuerzas armadas de países como Ecuador, Colombia o Perú mantienen para frenar al narcotráfico, como lo menciona Ricardo Cajas (2022).

La denominación de amenaza híbrida obedece a que estas organizaciones están conformadas por actores diversos (figuras políticas, públicas y/o privadas), empleando armas peculiares (bombas caseras, armas de fuego, etc.) y mecanismos diversos (panfletos, protestas sociales, noticias falsas o *fake news*, *trolls, bots*, etc.), puesto que combinan características de por lo menos dos amenazas diferentes (Bartolomé, 2019). En el presente caso de estudio se dejará en evidencia el empleo del metaverso y el espacio cibernético por parte de este tipo de amenazas.

Estas amenazas tienen la peculiaridad de actuar de forma enmascarada, dificultando al Estado el descubrimiento de sus actos ilícitos, debido a que han provocado una hibridación compleja de anticipar y de neutralizar (Argoti, 2022), donde los actos ilícitos se desarrollan en medio de actividades convencionales de la vida cotidiana o en medio de conflictos convencionales, y en la actualidad, incluso en el espacio cibernético a través de la *darkweb* y *deepweb*.

Entonces, al analizar el estado del arte disponible al respecto, se puede aseverar que estas amenazas híbridas también están empleando el metaverso como un centro de entrenamiento, o el espacio cibernético, como un centro de comercialización. Así también lo explica Oscar Balderas en su investigación denominada "Nación Criminal" (Balderas, 2022).

De esta manera, la literatura determina que las denominadas amenazas híbridas son estructuras que tienen la capacidad de emplear acciones coordinadas y sincronizadas, tanto de elementos convencionales como de los no convencionales, para de forma agresiva, paulatina, violenta e inverosímil, atacar deliberadamente

objetivos estratégicos y de alto valor, situados en diversas esferas (política, económica, militar, social, informativa, infraestructura y legal), como lo explica Collom-Piela (2019).

Nótese que estas amenazas híbridas envuelven al Estado en dilemas jurídicos que dificultan el empleo del poder nacional, y que incluso en ciertos casos el Estado se ve obligado a garantizar su normal desenvolvimiento de sus actividades, como es el caso de la protesta social, la movilidad humana, la migración, la seguridad de personas privadas de la libertad, el acceso a internet, entre otras.

Por tanto, es evidente que las amenazas híbridas también están actuando en el espacio cibernético y se enfrentan a un incipiente marco legal, condición que facilita su proliferación, incrementa su violencia, sus vínculos con el terrorismo y el narcotráfico.

Una vez que se ha analizado con mayor amplitud el concepto de amenaza híbrida y su accionar en el espacio cibernético, es oportuno puntualizar que estas amenazas se caracterizan por emplear ataques híbridos, mismos que mantienen como denominador común la capacidad de influenciar, corromper o enraizarse en los diferentes estratos de la sociedad, con énfasis en las estructuras de toma de decisiones (Estado u organización social).

Un capítulo aparte en el análisis de las amenazas híbridas contempla el estudio del narcotráfico, el cual posiblemente sea el principal motor para el nacimiento de estas amenazas. Por tanto, a continuación, se analizará su accionar en los últimos años y su afectación a la seguridad del Estado.

1.2. El narcotráfico y sus delitos conexos dentro y fuera del metaverso

El narcotráfico es una actividad criminal que consiste en la producción, manufactura, distribución, tráfico y venta ilegal de drogas prohibidas para el consumo humano. Los réditos económicos que se generan como parte de esta actividad han promovido la proliferación de una gran cantidad de crímenes conexos, tales como: el sicariato, la violencia, la corrupción, el blanqueo de dinero, el terrorismo y la trata de personas. En la actualidad, estos crímenes también están siendo perpetrados empleando medios digitales y el espacio cibernético, como se explicará más a detalle en las secciones subsiguientes del presente artículo.

La violencia es una de las principales formas de crímenes conexos que acompañan al narcotráfico. Esta violencia se puede presentar de muchas formas, desde la violencia física hasta la violencia económica, y hoy en día se evidencia la violencia no física a través de redes sociales y medios digitales, situación que limita aún más la capacidad del Estado para ejercer un control efectivo sobre estas actividades ilegales. Los narcotraficantes a menudo usan la violencia para controlar su territorio y mantener el control sobre los negocios ilegales, a través de asesinatos, secuestros, extorsiones (presenciales y virtuales) y ataques armados.

La corrupción es otra forma de crímenes conexos ligados al narcotráfico. Los narcotraficantes a menudo invierten en actividades como el soborno de funcionarios públicos, el lavado de dinero y el tráfico de influencias. Estas actividades le permiten al narcotráfico evadir la ley, operar con impunidad y controlar de forma indirecta el accionar del Estado a través de las economías políticas del crimen organizado, mencionadas por (Rivera-Rhon & Bravo-Grijalva, 2020). Incluso con el avance vertiginoso de las tecnologías de información y comunicación, las formas y medios de proliferación de corrupción conexa al narcotráfico son cada vez más impetuosas.

El blanqueo de dinero es otra forma de crímenes conexos relacionados con el narcotráfico. Esta actividad criminal, que es muy atractiva para muchos sectores de la sociedad, se refiere a la conversión de dinero obtenido de actividades ilícitas en dinero limpio y legítimo, en algunos casos, esto lo realizan a través del espacio cibernético. Esto se logra mediante el montaje de redes de comunicación virtual por medio de las cuales esta actividad se incrementa día a día. Así mismo, mediante la manipulación de registros financieros para ocultar el origen del dinero, por lo que, como menciona Galán-Gallegos (2005) al referirse a los acuerdos del Convenio de Viena de 1988, el objetivo es privar al narcotráfico de su rentabilidad.

El terrorismo también se ha convertido en un problema relacionado con el narcotráfico, y también está actuando en redes sociales y espacio cibernético (ONU, 2023), (Pons, 2017). Esto se debe a que los narcotraficantes a menudo proporcionan fondos a grupos terroristas para financiar sus actividades, con la finalidad de mantenerlos como su brazo armado, su muestra de poder. Esto se ha convertido en una gran amenaza para la seguridad en muchas partes del mundo (Gómez, 2023).

La trata de personas también está estrechamente vinculada al narcotráfico y también ha ampliado sus tentáculos a través del empleo del espacio cibernético (ONU, 2023). A menudo, los narcotraficantes explotan a las personas en situaciones de vulnerabilidad para usarlas como mano de obra barata para sus actividades ilegales. Esto puede incluir la producción y distribución de drogas ilegales, el tráfico de armas y el tráfico sexual (Redacción Plan V, 2021).

La situación geopolítica del Ecuador lo ha llevado a enfrentar los efectos colaterales de la siembra, cosecha y procesamiento de sustancias denominadas ilícitas, actividad que de forma paulatina y silenciosa se ha insertado en la sociedad ecuatoriana hasta alcanzar un punto en el cual hoy el Estado es considerado como parte de la cadena de valor del narcotráfico, y observa con dificultad e incertidumbre el empleo de la estrategia más adecuada para frenar actividades que han ido generando pánico en la sociedad, como es el caso de crimen organizado, entre otras (Rivera-Rhon & Bravo-Grijalva, 2020).

Nótese que este crimen organizado tiene un carácter de transnacional, puesto que se ha estructurado con miembros y organizaciones de diversa procedencia, sin encontrar una limitación en las fronteras físicas. Es decir, no encuentran limitaciones infranqueables, tanto para su organización como para su accionar, por tanto, el uso del espacio cibernético se ha convertido en una herramienta ideal para estas organizaciones. Pero, para configurar una organización de esta índole se requiere de un adecuado poder económico y de una forma precisa para ejecutar las transacciones requeridas, sin ser descubiertos (Rodriguez, 2006).

La estructura del narcotráfico se ha fortalecido con el establecimiento de alianzas criminales, como el caso de las FARC en Colombia, que luego del colapso de la URSS y la falta de recursos para financiar sus ilusiones políticas comenzaron a tener una relación de oportunidad con el narcotráfico para promover y respaldar sus actividades de: cultivo, producción de pasta, y en menor cantidad a la protección de los laboratorios, como lo afirma Ruiz (2017).

Sobre estos eslabones se establece un cobro a manera de impuesto, a cambio de permitir su funcionamiento y de prestar servicios de seguridad. En este sentido, las FARC captan recursos del narcotráfico desde los eslabones de producción, pues son ellos quienes cultivan y producen los estupefacientes (Cesare, 2015).

Tras la firma del acuerdo de paz entre el Estado colombiano y las FARC, a finales de 2016, Colombia experimentó una reducción en los niveles de violencia que generó sentimientos de esperanza. Sin embargo, la violencia regreso de la mano con el fortalecimiento de grupos armados no estatales en varias regiones del país, que tomaron el control de la producción, elaboración, transporte y envió de la droga, lo que llevo a alianzas con el crimen internacional como los carteles de Juárez, Tijuana, Sinaloa, Nueva Generación y del Golfo que extendieron sus tentáculos criminales hacia organizaciones insurgentes como las disidencias de las FARC, el Ejército de Liberación Nacional (en adelante, ELN), los grupos armados organizados (GAO) y bandas criminales (BACRIM) (Darío, 2020).

Lo anteriormente descrito amplía el contexto del accionar que provoca el narcotráfico, y como el crimen transnacional se ha ido involucrando como un eje fundamental, un socio estratégico o simplemente una actividad conexa que coadyuva a generar escenarios complejos para la seguridad del Estado; es así que, en Ecuador, en los últimos años se ha observado la presencia de organizaciones internacionales como el cartel de Sinaloa y el Cartel Jalisco Nueva Generación (CJNG), entre otros, las cuales han establecido alianzas con grupos criminales nacionales, como los tiguerones, los lagartos, los choneros y otros (Benavides & Guamán, 2023).

El establecimiento de alianzas criminales ha estado acompañada de actos ilícitos y violentos como robos, asesinatos, lavado de dinero, comercio de sustancias ilícitas, extorsiones, corrupción, entre otros; afectando el desarrollo integral del Ecuador, y de esta manera vulnerando el sistema de seguridad ecuatoriano (Benavides & Guamán, 2023), dejando en la sociedad una estela de inseguridad que limita su normal desenvolvimiento, que incluso está promoviendo la emigración.

Es trascendental considerar que esta amenaza para el Estado tiene una influencia importante sobre la sociedad en su conjunto, alcanzando en algunos casos una aceptación ─motivada o no─ para contribuir en actividades como el lavado de activos que derivan en once tipos de delitos conexos que amenazan al Ecuador, como es el narcotráfico, corrupción, captación ilegal de dinero, robo de vehículos, esquemas piramidales, trata de personas, delitos ambientales, préstamos extorsivos, usura, contrabando y evasión fiscal; así lo menciona un estudio de la Unidad de Análisis Financiero y Económico (UAFE) y la Organización de los Estados Americanos (OEA) (Gabriela, 2022).

La expansión del narcotráfico y su afectación a la seguridad ha llegado inclusive a las instituciones que deben combatirlo, siendo el caso más sonado el de los "narcogenerales", donde el embajador de Estados Unidos en Ecuador, Michael Fitzpatrick, calificó como "narcogenerales" a altos funcionarios de la Policía Nacional, acusándoles de estar utilizando dinero robado al pueblo ecuatoriano para vivir en Estados Unidos, por lo que informó que más de 300 visas, tanto de generales como de sus familiares, fueron retiradas a ciudadanos ecuatorianos investigados por delitos de corrupción (Ana C., 2021).

Todo esto permite catalogar al narcotráfico como un fenómeno que ha logrado adquirir un importante rol en varias dimensiones del Estado, como la dimensión económica, política y social, permitiendo que los grupos criminales tengan una organización más sistémica, donde se construyen alianzas nacionales e internacionales para alcanzar nuevas capacidades y motivaciones que conllevan a los Estados a la necesidad de catalogarlos como una gran amenaza no solo para el país y la región, sino para el mundo en general.

Entonces, se puede preguntar, ¿por qué es tan complejo para el Estado enfrentar estas organizaciones? Posiblemente, una de las respuestas sería porque las organizaciones están empleando varias estrategias y formas de comunicación, como el espacio electromagnético y cibernético, espacios que luego de la crisis sanitaria han tenido un empleo masivo, y más de 4.600 millones de personas en el mundo acceden a Internet, cifra que se incrementó en aproximadamente un 27%, a partir del aparecimiento del Covid-19 (Juste, 2023). Agentes que rastrean este tipo de delitos saben que las cibermafias apuestan por cuatro formas de operar. La más común se conoce como *phishing*[1], además se

1 Phishing es el delito de engañar a las personas para que compartan información confidencial como contraseñas o números de tarjetas de crédito

realizan infecciones digitales a computadores, creación de webs y plataformas fraudulenta, *hackean*[2] cuentas de redes sociales, provocando una alteración de la sociedad y un ambiente de pánico y miedo (Rosero, 2022).

Los ataques de las cibermafias son recurrentes en el país. Un informe estadístico de la Unidad de Ciberdelitos de la Policía muestra que en tres años (2020-2022) se han registrado 3.183 delitos informáticos. En el 2020 fueron 682 casos; en el 2021 subieron a 1.851 y hasta julio de 2022, la Policía inició 650 investigaciones a escala nacional (Redacción seguridad, 2022).

Este tipo de delitos, que ocurren en el citado espacio cibernético bajo denominaciones de *darkweb, deepweb* y *darkverse* (por citar algunas), y que justamente son de compleja detección para el Estado, son evidencias que muestran la capacidad de las nuevas amenazas a la seguridad del Estado y serán analizadas y estudiadas con mayor profundidad en el desarrollo de este artículo.

1.3. La *darkweb* y el narcotráfico

La *darkweb*, intuitiva y fácilmente traducida como web obscura, fue una herramienta creada en Estados Unidos como un medio para facilitar el intercambio de información entre agencias estatales, en especial, aquella información de inteligencia que resulta de importancia trascendental para el Estado y que debía ser adecuadamente protegida, a esta herramienta la denominaron como TOR (Sanz, 2019).

Para entender con mayor precisión el accionar de la *darkweb* es importante señalar que cuando un usuario emplea el internet y realiza sus consultas, estas actividades no tienen una sola dimensión, sino que pueden ser desarrolladas en otros ámbitos, de forma específica, en tres planos, cada uno de ellos con sus respectivas características y seguridades.

En el primer plano, se encuentra la web superficial, que es la porción de internet cuya información está indexada por los motores de búsqueda y que es accesible a través de los navegadores y buscadores tradicionales (Internet Explorer, Google Chrome, Firefox u otros), de forma abierta y gratuita, que no requiere mayor conocimiento ni requisitos para el usuario o individuo que requiere acceso a la información.

En segundo lugar, se encuentra la web profunda, que es la parte de internet cuyos contenidos no pueden ser indexados abiertamente por los buscadores tradicionales, aquí se ubica la información y los datos que están protegidos por contraseñas y que pertenecen a agencias gubernamentales, bibliotecas o universidades, los cuales mantienen ciertas restricciones para su acceso y difusión.

En tercer lugar, se encuentra la web oscura, que es una pequeña parte de la web profunda, la cual tampoco está indexada por los motores de búsqueda; pero que, a diferencia de la web profunda, es restringida. Así, la web oscura o darkweb es una porción de la web que se ocultó intencionalmente y a la que solo se puede llegar a través de programas tales como, Tor browser, el cual permite acceder a la red Tor (García, 2017).

Por tanto, colocar información en la web tiene varias implicaciones y requerimientos, que deben ser adecuadamente conocidos por los usuarios, en especial, aquellos que requieren administrar información que demanda un tratamiento y sigilo adecuado, puesto que su difusión puede provocar violaciones a la seguridad de la sociedad y la nación en su totalidad.

Para tomar conciencia de la magnitud de esta parte de la web, es oportuno señalar que la darkweb es 500 veces más grande que la web superficial y también que, por la magnitud de la información que almacena, los 60 sitios más importantes de la *deepweb* tienen 40 veces mayor capacidad de almacenamiento que todos los sitios de la web superficial (García, 2017).

Así mismo, es sustancial señalar que la *darkweb* no es un sinónimo absoluto de ilegalidad, y que, por el contrario, tiene una utilidad importante para permitir una comunicación protegida (García, 2017).

Pero este lado del anonimato en el que se enmarca la *darkweb* ha traspasado los límites y las buenas intenciones por las que fue creada, y ha dado paso a que se emplee como una plataforma conveniente para la ejecución de actividades criminales de organizaciones terroristas, narcotraficantes, traficantes de armas, sicarios, vendedores de información robada, pedófilos entre otros.

En la *darkweb* los delincuentes pueden ocultar su identidad y evitar la detección policial y/o de las entidades de control del Estado, lo que hace que sea un lugar ideal para el crimen organizado, quienes, a cuenta de esta fragilidad legal continúan incrementando sus ganancias (García, 2017).

Actualmente, muchas organizaciones consideran a los datos como uno de sus activos más valiosos. Si estos no están bien protegidos, pueden convertirse en un problema o una amenaza, al poner en riesgo la identidad e intimidad de personas y resultar en una crisis reputacional. De acuerdo con McAfee, en el primer trimestre de 2019, los secuestros de datos (*ransomware*)[3] crecieron un 118% y se detectaron nuevas e innovadoras técnicas para los ataques.

Es importante comprender que, en la realidad virtual, los atacantes pueden contar con diversos perfiles. Pueden ser empleados de un Estado-nación, miembros de un grupo criminal organizado o solo usuarios curiosos en la búsqueda de información. No obstante, los tres comparten el mismo rasgo: la intención de aprovechar las brechas en la estrategia de seguridad de las organizaciones, personas, empresas o entidades estatales; en algunos casos, para causar estragos en los

2 Hackeo consiste en poner en riesgo sistemas informáticos, cuentas personales, redes de ordenadores o dispositivos digitales para obtener información.
3 El ransomware, en informática, es un tipo de malware o código malicioso que impide la utilización de los equipos o sistemas que infecta. El ciberdelincuente toma control del equipo o sistema infectado y lo "secuestra" de varias maneras, cifrando la información, bloqueando la pantalla, etc.

negocios y operaciones; y en otros con un objetivo más explícito: robar los datos.

De acuerdo con el Reporte Anual de Cibercrimen realizado por Cybersecurity Ventures, el cibercrimen le costó al mundo 6 billones de dólares. Según el informe, esto representa la mayor transferencia de riqueza económica en la historia y pone en riesgo los incentivos para la innovación y la inversión. Igualmente, el reporte alarma que el cibercrimen será el negocio más rentable en el mundo; aún más que el comercio global combinado de las principales drogas ilegales. El robo de datos fomenta daños, destrucción, pérdida de productividad, fraude, malversación de fondos o robo de dinero, etc. (Bussines empresarial, 2020).

Entonces, el Estado debe ir incrementando su capacidad de actuar en todos los ámbitos que la necesidad así lo requiera para poder garantizar su soberanía y el ambiente de paz y desarrollo que constitucionalmente así lo establece. Por tanto, debe ser capaz de actuar en este ámbito que traspasa fronteras y en donde el crimen organizado ha encontrado un asidero para incrementar su potencial capacidad.

Hoy se observa con preocupación como este escenario web creado para garantizar seguridad, por el contrario está facilitando la forma de comunicación de las organizaciones ilegales, las cuales emplean sistemas encriptados[4] que enmascaran sus mensajes, como sucedió en marzo del 2021, en el caso Dossier Sky ECC llevado a cabo por la Europol[5], en Bélgica y Francia, con el registro y análisis de más de mil millones de mensajes que intercambiaban información entre grupos criminales de 22 países catalogados como productores, puntos de tránsito y distribución de cocaína. Aquí se verificó la existencia de términos como *mocromafia* (traficantes de origen marroquí que operan desde Países Bajos) y la *ndragheta calabresa* (mafia napolitana) (swissinfo, 2022).

Las consecuencias de la infiltración y robo de información no se encuentran solo direccionadas hacia Estados Unidos y los países europeos, ya que al no tener el internet una frontera definida, permite al crimen organizado actuar desde cualquier lugar y en cualquier momento.

Ecuador no queda exento de estos ataques, como lo muestra la experiencia vivida en septiembre del 2019, donde la compañía de seguridad informática VPNMentor aseguró en un informe que dos de sus expertos detectaron que una empresa de análisis de datos que no contaba con los protocolos de protección necesarios sufrió un hackeo de 18 GB de datos distribuidos en una variedad de archivos, que incluía nombres, información financiera y datos civiles de hasta 20 millones de personas.

Estos eventos evidencian la fragilidad y vulnerabilidad que existe en el Ecuador en este ámbito, y que pone en riesgo información importante. El objetivo del robo de datos es obtener información personal, financiera o comercial para usarla con fines fraudulentos, como el robo de identidad, el fraude bancario, el fraude de tarjetas de crédito y de cuentas de correo electrónico. Los delincuentes también pueden vender los datos robados a terceros, generalmente en el mercado negro de la darkweb, para obtener un beneficio económico o un intercambio de beneficios (BBC News Mundo, 2019).

Aunque todo este tipo de delitos utiliza la *darkweb* para expandir su negocio, también se vuelve necesario su implementación en la economía real, para el incremento de ganancias, así se puede notar que en el Ecuador se ha penetrado principalmente en las microfinanzas, donde no llegan los servicios institucionales como bancos y cooperativas, lo que ha permitido que el narcotráfico y esquemas de corrupción participen en la captación ilegal de dinero, la usura y la estafa.

El problema con la captación ilegal es que las personas sacan sus recursos de las instituciones financieras autorizadas y las destinan a supuestas entidades que ofrecen pagar intereses más elevados, causando una vulneración de la capacidad de control de Estado, y provocando la proliferación de actividades ilegales que terminan con cruces de cuentas, muertes violentas, entre otros.

Uno de ellos fue el sonado esquema Ponzi[6] "Big Money", cuya cara más visible era Miguel Ángel Nazareno, un exmilitar que incrementó exponencialmente su red, a través del presunto pago de intereses de 90% en ocho días (Gabriela, 2022). Como se evidencia, los tentáculos del narcotráfico son amplios, y la seguridad del Estado percibe una afectación crítica, pues la capacidad de control es incipiente. Finalmente, como es de conocimiento público, Miguel Nazareno fue asesinado, dejando un vacío de información importante para el Estado.

2. EL METAVERSO COMO UNA AMENAZA A LA SEGURIDAD

Un metaverso es en esencia un espacio social en un mundo virtual, cuyos escenarios son desarrollados en tercera dimensión. Puede ser concebido como una infraestructura canalizada a través de una red inteligente que mediante un sistema de inteligencia artificial (IA), genera datos en tiempo real y provoca sensaciones diversas para cada usuario conectado al mismo (Meta, 2022).

En realidad, este concepto no es totalmente inédito o novedoso como parecería, ya que desde hace tiempo existe un buen número de metaversos, principalmente

4 La encriptación es una forma de codificar los datos para que solo las partes autorizadas puedan entender la información.
5 Policía europea
6 El esquema Ponzi es una operación fraudulenta de inversión que implica el pago de intereses a los inversores de su propio dinero invertido o del dinero de nuevos inversores, que caen engañados por la promesa de obtener grandes beneficios.

en el sector de los videojuegos, dónde su evolución ha sido un espacio de prueba para el desarrollo de nuevas capacidades.

Sin embargo, por diversas causas, el metaverso ha permanecido en una pausa, y gracias al reciente auge de distintas tecnologías, la capacidad de acceso al internet, que en Ecuador supera el 70% y en el mundo supera el 62% (Banco Mundial, 2022) (Juste, 2023), las expectativas para explotar el metaverso son mayores y han evolucionado más allá de un escenario de juego y/o educación (López, Álvarez, & Carrasco, 2022).

En términos generales, si se busca una simplificación conceptual, los campos que actualmente se ven más beneficiados con el desarrollo del metaverso son: el campo social, el educativo, el entretenimiento, la actividad física, la superación personal, el comercio, entre otros (Meta, 2022), y esto sucede debido a que en los campos expuestos se ha visualizado la importancia y efectividad que tiene la realidad virtual y como, por intermedio de este pilar básico del metaverso, se pueden mejorar estándares de rendimiento, producción, etc.

Al analizar la perspectiva histórica, se podría señalar que la definición de metaverso nace de la novela de ciencia ficción Snow Crash, creada y publicada por Neal Stephenson en 1992, donde no se lo define como una evolución de la realidad virtual, sino como una recreación de realidades que van más allá de una imaginación virtuosa. El metaverso es visualizado como un entorno de convivencia en línea, en el que los usuarios consideran a este como un lugar real, e interactúan utilizando el mundo real como metáfora y articulan nuevos grupos sociales, realizan negocios o se divierten creando una vida paralela (Ávila, 2022).

En la actualidad, grandes empresas como Coca-Cola, Nike, Hyundai, Facebook, WhatsApp, Messenger, Instagram, entre otras, son parte activa del metaverso, creando escenarios virtuales y una interacción permanente con actores empresariales y con clientes, quienes contribuyen con ideas, alternativas y propuestas innovadoras que orientan el futuro operativo y comercial de estas instituciones (Bello, 2022).

Es decir, de cierta forma esta interacción que oferta el metaverso permite una generación de una participación colectiva y colaborativa, que es aprovechada por los líderes empresariales para promover innovación y evolución de su industria.

Posiblemente esta participación colectiva esté generando recursos a las industrias, sin que estos reconozcan a los verdaderos autores y ponentes de estas ideas innovadoras, por tanto, se estaría violentando e irrespetando los derechos de propiedad intelectual, y hasta de relación laboral, un aspecto que debe ser analizado también por los diversos Estados.

El metaverso se le puede considerar una evolución dentro del internet a las redes sociales, ya que, aunque nace desde el concepto de lo social, también tiene diferencias marcadas con las redes sociales como Facebook, Instagram, Whatsapp, entre otras. Estas diferencias son:

1. El metaverso se basa en un mundo virtual, mientras que las redes sociales se basan en la interacción social real.
2. El metaverso ofrece una variedad de herramientas de construcción de mundos virtuales, mientras que las redes sociales ofrecen herramientas para conectar a las personas.
3. El metaverso permite a los usuarios interactuar con los entornos virtuales creados, mientras que las redes sociales permiten a los usuarios compartir contenido.
4. El metaverso ofrece la libertad de crear entornos virtuales personalizados, mientras que las redes sociales están limitadas por las opciones de configuración de la plataforma.
5. El metaverso permite a los usuarios construir sus propios mundos y experiencias, mientras que las redes sociales se limitan a la interacción entre usuarios (Paola, 2021).

Todas las implicaciones del metaverso como un mundo virtual conllevan a que se desarrolle en muchos ámbitos a la par de los que existen en la vida real, siendo los más importantes para nuestro estudio el metaverso militar, financiero e industrial. Es pertinente también, referirse al metaverso policial como una innovación lanzada por la Interpol para enfrentar las nuevas amenazas (Interpol, 2023), y cuyo objetivo principal es investigar delitos como: *ransomware*, lavado de activos, acoso sexual, fraude financiero, *pishing*, entre otros.

2.1. El metaverso militar

Al analizar la definición, alcance y contexto general del metaverso, se puede observar que este ambiente proporciona una amplia factibilidad para explotar estas capacidades y bondades en el ámbito de la formación, de la capacitación, del perfeccionamiento, del entrenamiento, y porque no decirlo, del empleo del poder militar en situaciones en que así sea requerido.

Las bondades del metaverso y la poca explotación del mismo por parte de los organismos de control, conciben la necesidad de implementar ciertas adaptaciones y configuraciones a fin de garantizar la seguridad de la información que sea puesta sobre las diferentes plataformas empleadas en este ámbito, es decir, emplear los conceptos y capacidades descritas en la segunda sección del presente artículo.

Por tanto, es evidente que la definición primaria de metaverso ha alcanzado una proyección hacia el mundo militar, dando origen al metaverso militar, mismo que, contradictoriamente a los afirmado por Ávila (2022), se dice que nació en 1978,¿ cuando el Capitán Jack Thorpe, miembro de la Fuerza Aérea de Estados Unidos (USAF), concibió la idea de usar simuladores de vuelo para la planificación, el ensayo y la ejecución en el combate, lo que llevó a finales de la década de los 80 al programa SINMET, ejecutado por el Departamento de Investigación de Proyectos Avanzados

de los EE.UU. (DARPA), y que entre sus objetivos buscó la construcción de un sistema de simuladores de conducción y empleo de tanques y aviones, mismo que interactuaban en escenarios geográficos distantes (EE. UU. y Europa) y que cumplían operaciones combinadas.

A principios de la década de los noventa, DARPA implementó una red de datos entre el navío multipropósito de asalto anfibio USS Wasp, en el puerto de Norfolk Virginia y los helicópteros simulados SINMET del Cuerpo de Marines en Fort Rucker, Alabama, en cuya red también existían tanques simulados, centros de comando del personal de la marina y un nodo de observación en el instituto de análisis de la defensa, materializando así un escenario virtual que se constituyó en el primer metaverso militar.

Después del SINMET, los militares pertenecientes a la Organización del Tratado del Atlántico Norte (OTAN) continuaron adoptando la idea de que los mundos real y virtual convergen en la doctrina y en el empleo operativo, es así que el Ministerio de Defensa del Reino Unido estableció un concepto para los denominados entornos sintéticos, definidos como la "vinculación de una combinación de modelos, simulaciones, personas y equipos reales en una representación común del mundo que proporciona coherencia y simultaneidad entre actividades previamente descritas" (Radar, 2022).

Esta posibilidad de usar el mundo virtual para simular el espacio de batalla llevó al Reino Unido a desarrollar la idea de un "gemelo digital" del mundo real, con igual complejidad y realismo que se convertía en un medio para aprovechar el desafío, visualizar y transformar el apoyo en la toma de decisiones, y así facilitar el acceso a modelos y datos en toda la simulación de la operación a ser ejecutada (Alfonso, 2018).

Todo este desarrollo ha llevado al uso de estándares de interoperabilidad entre los simuladores militares, a fin de mejorar la experiencia de entrenamiento para su uso en el mundo real, e incrementar el profesionalismo a través del uso compartido de plataformas tecnológicas que facilitan el aprendizaje y entrenamiento. Si bien es cierto, los entornos simulados no podrán reemplazar íntegramente a los escenarios reales, estas simulaciones incrementan las destrezas y habilidades en el uso de determinados sistemas de una manera efectiva.

Actualmente, muchas fuerzas militares procuran enfrentar con oportunidad y proactividad este desafío tecnológico de implementar mundos virtuales en tres dimensiones que, a pesar de su aparente impacto táctico y operativo, tienen consecuencias estratégicas para el Estado, puesto que incrementan su capacidad de respuesta.

Estos mundos virtuales deben permanecer conectados en red y potenciar la característica de actuación inmersiva, característica que contribuye a la generación de escenarios con elevada semejanza a la realidad. Condición que permite una mejor adaptación a entornos diferentes, un mejor planeamiento y ejecución de la conducción militar y la consecución de los objetivos políticos, estratégicos y operacionales (Herrera, 2021).

Por su parte, en el Ecuador se ha observado una suma de esfuerzos importantes por desarrollar un metaverso militar, mismo que ha dado sus primeros pasos a través de la investigación realizada en la Universidad de las Fuerzas Armadas - ESPE, específicamente en el Centro de Investigación de Aplicaciones Militares CICTE, donde se han implementado una base importante de simuladores que permiten el entrenamiento virtual de los miembros de FF.AA., a saber: simulador de vuelo y desorientación espacial de vuelo, simulador de paracaidismo, asistente virtual para áreas médicas y servicios universitarios; por tanto, esta base constituye un punto de partida importante hacia el metaverso militar.

Sin embargo, el desarrollo alcanzado debe ser transformado y potenciado, a fin de elevar la simulación de los enfrentamientos convencionales, a un nivel de extrema semejanza, y que extrapole también su doctrina de empleo al ambiente urbano, a la capacidad de enfrentar amenazas híbridas y asimétricas y al accionar ante las protestas sociales. Además, que sea capaz de realizar entrenamientos combinados con otras instituciones nacionales e internaciones que permitan manejar doctrinas convergentes y explotar las bondades que brinda el metaverso y el espacio cibernético.

Por otro lado, la estructura educativa de FF.AA. debe armonizar estos esfuerzos y capacidades alcanzadas y potenciales, para amalgamarlas en un enfoque convergente de construcción de un sistema institucional de entrenamiento virtual que permita no únicamente el entrenamiento aislado, sino que fomente un entrenamiento interagencial, para de esta forma desarrollar la capacidad de operaciones conjuntas e interagenciales, cuyos resultados, sin duda serán más efectivos que el de operaciones únicamente coordinadas.

2.2. Metaverso financiero

Las redes sociales, el mercado financiero y las experiencias digitales revolucionaron la forma en la que muchas personas se relacionan y consumen. Sin embargo, las principales transformaciones vinculadas con la convergencia entre lo real y lo virtual se prevé que revolucionaran el mundo de la tecnología para los próximos años, con el perfeccionamiento y la expansión del metaverso.

Para las instituciones financieras, el metaverso representa un punto de inflexión estratégico y será responsable de acelerar algunas tendencias dirigidas al crecimiento demográfico de los millennials (personas nacidas entre 1980 y 1994) y de miembros de la generación Z (nacidos entre 1995 y 2020). Podemos ver que algunas instituciones financieras ya empezaron incluso a construir sucursales como es el caso de JP Morgan, que anunció la apertura de una sucursal en el metaverso (Forbes, 2022).

Estos mundos virtuales creados del metaverso, permitirán innumerables alternativas de negocio y formas de hacer dinero como el *gaming*, turismo, viajes,

arte, etc. Pero, así mismo surgen riesgos generados por la factibilidad de que personas inescrupulosas defrauden, estafen, roben o desfalquen a clientes que buscan bienes o diferentes servicios virtuales, y que deben ser debidamente controlados, regulados y monitoreados por el Estado.

2.3. Metaverso industrial

La tendencia tecnológica que dirigirá buena parte de la innovación durante las próximas décadas es la confluencia del mundo virtual y el físico, basado en un entorno virtual único para cada persona, que le permitirá al cliente diseñar, dirigir y hasta supervisar el desarrollo de su pedido de manera virtual, materializando una atención personalizada y más cercana al cliente (Rodríguez, 2022).

Todas estas realidades virtuales también permiten el fomento del crimen organizado, que ve oportunidades para desarrollarse y crecer, pero, sobre todo, porque podrán tener acceso a información fundamental para la seguridad o para el desarrollo de la manufactura, afectando así, a un sector de la sociedad que sostiene económicamente al país (LogisticsWorld, 2023). Por otro lado, pueden subrepticiamente interactuar en este mundo y aprovechar la capacidad de la industria, para fabricar productos que serán empleados en actividades ilegales.

2.4. El darkverse

El metaverso es uno de los conceptos que más revuelo ha causado en los últimos años con la comunidad de internet creciendo día a día y los cripto-entusiastas adoptando las criptomonedas[7] para sus usos cotidianos; sin embargo el metaverso también da la creación y evolución del *darkverse* o "universo oscuro", donde la delincuencia opera (HoyCripto, 2023).

Los investigadores de seguridad predicen que allí podría surgir una especie de estructura similar a la internet actual.

Los ciberdelincuentes ven al metaverso como una forma de:

- Lanzar ciberataques
- Lavar dinero
- Realizar campañas de desinformación

Esta nueva realidad permitirá incluso que los ciberdelincuentes tengan "salas vitruales protegidas"[8] a las que solo se puede acceder desde una ubicación física específica y mediante tokens[9] de autentificación válidos. Esto haría que sus mercados clandestinos fueran inaccesibles para las fuerzas del orden.

Estas amenazas que van evolucionando junto a la tecnología, han facilitado la estructuración de espacio cibernético denominado como el *darkverse*, mismo que se ha convertido en el nuevo refugio de la ley para los cibercriminales, los cuales de cierta forma están estrechamente ligados al crimen organizado y el narcotráfico, pues a través de estos financian sus actividades cibernéticas y promueven un crecimiento de las mismas, como lo refiere el estudio realizado por la compañía de ciberseguridad Trend Micro (Syntonize, 2022).

El *darkverse* se convierte en una fuerza oculta para las fuerzas del orden, la cual podría evolucionar rápidamente para alimentar una nueva industria de la ciberdelincuencia relacionada con el metaverso, en un ambiente adecuado para potenciar la creación de nuevos escenarios, de nuevas dimensiones de la vida humana. Esta evolución va relacionada principalmente con las siguientes presunciones:

- Los NFT[10] se verán afectados por el *phishing*, los rescates, los fraudes y otros ataques, que serán cada vez más afectados a medida que se conviertan en un importante bien del metaverso para regular la propiedad privada.
- El *darkverse* se convertirá en un importante espacio de investigación por parte de las entidades de control de un estado (permite monitoreo, rastreo e infiltración), dado que permite enfrentar con oportunidad al narcotráfico, el crimen organizado, y toda actividad que emplee este espacio, para ejecutar acciones que violentan la seguridad y poder del Estado.
- El blanqueo de capitales mediante el uso de bienes inmuebles sobrevalorados en el metaverso y NFT, proporcionarán una nueva salida a los delincuentes para limpiar el dinero que se emplean en la transacción del narcotráfico y sus delitos conexos.
- La ingeniería social, la propaganda y las *fake news* tendrán un profundo impacto en un mundo ciberfísico. Los delincuentes y los agentes estatales emplearán narrativas influyentes y convincentes dirigidas a grupos vulnerables y sensibles a determinados temas.
- Los ciberdelincuentes buscarán comprometer los "gemelos digitales" gestionados por operadores de infraestructura crítica de los estados, para lanzar ataques y sabotear o extorsionar los sistemas industriales, provocando una grave afectación al desarrollo en todo su contexto (Dominguez, 2022).

Por lo pronto, esta mueva evolución tecnológica, actualmente aparentemente incipiente como el darkverse, con el pasar el tiempo se volverá un motor

7 Una criptomoneda es un activo digital que emplea un cifrado criptográfico para garantizar su titularidad y asegurar la integridad de las transacciones para evitar que alguien pueda hacer copias y así poder ser usado como moneda digital.

8 La sala virtual es un espacio virtual que dispone de un identificador único (dirección de acceso), que le permite al organizador de una reunión, invitar participantes de distintas ubicaciones geográficas para que se conecten en tiempo real usando el internet.

9 Token es un código de seguridad, emitido por una entidad privada y solo es válido en un contexto virtual específico.

10 Los NFTs o Token no fungibles (Non Fungible Token en inglés) son activos digitales certificados como únicos y que pueden ser comprados por una persona para ser su propietario.

dinamizador de economía, de actividades ilegales y que demandará un control masivo y efectivo para frenar la criminalidad, el tráfico de bienes; y toda aquella actividad que violente la seguridad del Estado, por tanto, las entidades de control y las de seguridad deben actuar de forma mediata para evitar la sorpresa por parte de los grupos ilegales.

CONCLUSIONES

En el corto plazo, el incremento de la capacidad de las amenazas híbridas para explotar el espacio cibernético afectará significativamente a la seguridad del Estado, con énfasis a la infraestructura crítica y tecnológica de varias entidades, generando afectaciones muy graves a la sociedad y/o al Estado, puesto que en la actualidad toda institución pública depende en gran parte de las tecnologías de información y comunicación, de las redes de datos y de las transacciones digitales.

El fácil acceso a los servicios y plataformas web (más de 4.600 millones de usuarios de Internet), y la tendencia a un mundo totalmente digital, masifica las actividades en el metaverso, *darkweb* o *deepweb*, dando la oportunidad de mayor ocurrencia de acciones ilegales, y la consecuente afectación a la seguridad integral del Estado, pues las acciones de control en este ámbito son muy complejas, incluso si se lograse disponer de la infraestructura más moderna y segura.

Es fundamental que el Estado defina una entidad (FF.AA. por ejemplo) que lidere la materialización de proyectos de ley integrales y resilientes, para que las políticas de ciberseguridad que actualmente dispone el Ecuador se materialicen en una capacidad operativa efectiva para prevenir, investigar, combatir y neutralizar las amenazas originadas en el espacio cibernético y el metaverso, debido a que las acciones aisladas que realicen las instituciones, nunca podrán tener el impacto requerido ante una amenaza que podría definirse como abstracta, pero cuyas acciones tienen consecuencias no abstractas y muy perjudiciales para la sociedad.

Internacionalmente se observa que varias entidades están visualizando al metaverso como un potencial de desarrollo, crecimiento y visión prospectiva para enfrentar nuevos escenarios. En ese contexto, se evidencia el desarrollo de metaversos militares, policiales y educativos; por tanto, el Ecuador debe permanecer con una actitud estratégica proactiva y de permanente evolución que genere soluciones oportunas y una ingente capacidad de respuesta ante estos eventos, alcanzado un Ecuador digital ciberseguro, con capacidad de garantizar el estado de derecho de la población.

Referencias

Accessnow. (11 de ene de 2023). *Disrupciones de internet en Ecuador: cómo ocurrieron y cómo eludirlas.* https://www.accessnow.org/disrupciones-de-internet-en-ecuador-como-ocurrieron-y-como-eludirlas/

Alfonso, M. (2018). ¿ Qué es un Digital Twin o gemelo digital y de dónde vienen? *Byte España,* (266), 48-58.

Ana, C. (13 de diciembre de 2021). www.cnnespanol.com. https://cnnespanol.cnn.com/2021/12/13/eeuu-narcotrafico-ecuador-orix/

Argoti, M. (2022). La estrategia contra las amenazas híbridas. *Revista de la Academia de Guerra del Ejército Ecuatoriano, 15*(1), DOI: https://dx.doi.org/10.24133/age.n15.2022.12, 151-164.

Ávila, J. (2022). World Compliance Association. https://worldcomplianceassociation.com/3050/articulo-el-metaverso-conceptualizacion-juridica-retos-legales-y-deficiencias-normativas.html

Balderas, O. (Dirección). (2022). *Nación Criminal: Interpol irrumpe en el metaverso* [Película].

Banco Mundial. (10 de ene de 2022). Personas que usan internet en el Ecuador. https://datos.bancomundial.org/indicator/IT.NET.USER.ZS?locations=EC&name_desc=true

Barreno-Jardi, C. (2011). Zygmunt Bauman y la Sociedad Líquida. Esfinge.

Bartolomé, M. (2019). Amenazas y conflictos híbridos: características distintivas, evolución en el tiempo y manifestacoines preponderantes. *URVIO*, 25, E-ISSN 1390-4299 ISSN 1390-3691, 8-23.

BBC News Mundo. (15 de septiembre de 2019). www.bbc.com. www.bbc.com: https://www.bbc.com/mundo/noticias-america-latina-49721456

Bello, E. (10 de nov de 2022). *Siete ejemplos de empresas y marcas que ya han abrazado el metaverso*. https://www.iebschool.com/blog/ejemplos-empresas-metaverso-tecnologia/

Benavides, M., & Guamán, M. (20 de ene de 2023). *Seguridad y crimen transnacional: La geopolítica del narcotráfico como amenaza a la seguridad del Estado*. www.puce.edu.ec: http://repositorio.puce.edu.ec/bitstream/handle/pdf?sequence=1&isAllowed=y

Bussines empresarial. (20 de enero de 2020). www.businessempresarial.com.pe. https://www.businessempresarial.com.pe/el-robo-de-datos-un-negocio-lucrativo/

Cajas, R. (2022). Las amenazas híbridas, un nuevo reto para los Estados. *Revista de la Academia de Guerra del Ejército Ecuatoriano,15*(1), DOI: https://dx.doi.org/10.24133/age.n15.2022.02 , 29-62.

Cesare, B. (2015). www.dialnet.unirioja.es. www.Dialnet-ElNarcotrafico-5627079-3.pdf

Colom-Piella, G. (2012). Vigencia y limitaciones de la guerra híbrida. *Revista Científica "General José María Córdova", 10*(10), ISSN 1900-6586, 77-90.

Colom-Piella, G. (2019). *La amenaza híbrida: mitos, leyendas y realidades.* Instituto de Estudios Estratégicos de España.

Constitución de la República del Ecuador, Registro Oficial Nro. 449, del 20 de octubre del 2008. (2008).

Darío, C. (10 de abril de 2020). http://www.scielo.org.co. http://www.scielo.org.co/pdf/njus/v14n2/2500-8692-njus-14-02-123.pdf

Dominguez, M. (16 de septiembre de 2022). www.cybersecuritynews.es. https://cybersecuritynews.es/ciberamenzas-en-un-metaverso-oscuro/

Forbes. (17 de febrero de 2022). www.forbes.com.ec. https://www.forbes.com.ec/negocios/jp-morgan-ya-tiene-su-sucursal-metaverso-puede-hacer-ella-n12815

France24. (11 de ene de 2022). *Narco, crimen y protestas: Ecuador vuelve a mirar al abismo.* https://www.france24.com/es/minuto-a-minuto/20211024-narco-crimen-y-protestas-ecuador-vuelve-a-mirar-al-abismo

Gabriela, C. (2025 de junio de 2022). www.primicias.ec. https://www.primicias.ec/noticias/economia/narcotrafico-captaciones-ilegales-amenazas-microfinanzas/

Galán, C. (2018). *Amenazas Híbridas: nuevas herramientas para viejas aspiraciones*. Real Instituto Elcano, 3.

Galán-Gallegos, H. (2005). *Narcotráfico y Blanqueo de Capitales: un problema internacional.* Anuario de la Facultad de Derecho, 213-226.

García, L. (2017). Narcotráfico en la Darkweb:los criptomercados. URVIO, *Revista latinoamericana de Seguridad*, 191-206.

Gómez, A. (20 de ene de 2023). Unirioja. *Terrorismo, narcotráfico y conflicto en el caso colombiano.* La cooperación internacional: https://dialnet.unirioja.es/descarga/articulo/1977933.pdf

Herrera, O. (2021). El Metaverso ¿Una construcción del Ejército? *Pensamiento Conjunto*, 4-8.

Interpol. (20 de ene de 2023). *Interpol lanza el primer metaverso policial del mundo*. https://www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2022/INTERPOL-lanza-el-primer-metaverso-policial-mundial

Juste, M. (21 de ene de 2023). *La pandemia dispara el uso de las redes sociales, un 27% más que hace un año.* Expansión.com: https://www.expansion.com/economia-digital/novacion/2021/02/10/6022c89de5fdea59448b459b.html

Ley de Seguridad Pública y del Estado, R. O.-s.-2. (2009, modificada en 2014). Quito.

LogisticsWorld. (20 de ene de 2023). *5 formas en que el metaverso industrial afectará a los fabricantes*. https://thelogisticsworld.com/manufactura/5-formas-en-que-el-metaverso-industrial-afectara-a-los-fabricantes/

López, C., Álvarez, P., & Carrasco, A. (14 de febrero de 2022). GA_P. Gómez-Acebo&Pombo Abogados: https://www.ga-p.com/publicaciones/que-es-el-metaverso/

Meta. (20 de nov de 2022). *Cómo estamos creando el metaverso*. https://about.meta.com/ltam/meta/

Ministerio de Defensa Nacional. (sep de 2019). *Plan Estratégico Institucional de Defensa 2017-2021*. https://www.defensa.gob.ec/wp-content/uploads/downloads/2021/04/PEI-2017-2021_revista_act_2021.pdf

ONU. (20 de dic de 2023). Organización de las Naciones Unidas. *Las redes sociales, la principal arma terrorista durante la pandemia de COVID-19*: https://news.un.org/es/story/2020/11/1484342

ONU. (20 de ene de 2023). Organización de las Naciones Unidas. *La trata de mujeres y niñas se extiende al ciberespacio por medio de las redes sociales*: https://news.un.org/es/story/2020/11/1483922

Paola, R. (17 de noviembre de 2021). www.le-vpn-com. https://www.le-vpn.com/es/metaverso/

Policía Nacional. (14 de ene de 2023). *Delitos informáticos o Ciberdelitos*. https://www.policia.gob.ec/delitos-informaticos-o-ciberdelitos/

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

Radar, E. (20 de nov. de 2022). *Entornos sintéticos: la clave del realismo en el adiestramiento militar*. https://www.elradar.es/entornos-sinteticos-la-clave-del-realismo-en-el-adiestramiento-militar/

Redacción Plan V. (21 de agosto de 2021). www.planv.com.ec. https://www.planv.com.ec/historias/sociedad/ecuador-radiografia-del-crimen-organizado-y-sus-actores

Redacción seguridad. (25 de julio de 2022). www.elcomerico.com. https://www.elcomercio.com/actualidad/seguridad/3183-delitos-informaticos-se-han-registrado-en-el-ecuador-desde-el-2020.html

Rivera-Rhon, R., & Bravo-Grijalva, C. (2020). Crimen Organizado y cadenas de valor: el ascenso estratégico del Ecuador en la economía del narcotráfico. URVIO, *Revista Latinoamericana de Seguridad y Defensa*, 28, 8-29.

Rodriguez, A. (. (2006). El narcotráfico como crimen organizzado trasnacional desde una perspectiva criminológica. Capitulo criminológico: *Revista de las disciplinas del control social, 27.*

Rodríguez, J. (21 de julio de 2022). www.forbes.com.ec. https://www.forbes.com.ec/innovacion/el-metaverso-empresas-futuro-mito-o-realidad-n19191

Rosero, A. (11 de enero de 2022). www.elcomercio.com. https://www.elcomercio.com/actualidad/seguridad/ciberdelincuencia-ecuador-organizaciones-delictivas-victimas.html

Ruiz, F. (2017). La internacional terrorista patrocinada por la URSS. *Revista Contribuciones a las Ciencias Sociales.*

Sales, A. (10 de oct de 2019). *La amenaza híbrida: la guerra imprevisible.* https://www.unav.edu/web/global-affairs/detalle/-/blogs/la-amenaza-hibrida-la-guerra-imprevisible#

Sanz, M. (22 de jun de 2019). Qué es y como funciona la darweb. *Computer:* https://computerhoy.com/reportajes/tecnologia/consiste-dark-web-441771

SNGR. (12 de ene de 2023). Secretaría Nacional de Gestión de Riesgos. *Plan Estrtégico Institucional 2021-2025:* https://www.gestionderiesgos.gob.ec/wp-content/uploads/downloads/2022/02/PEI-SNGRE-2021-2025-28-12-21-F.pdf

Syntonize. (10 de dic de 2022). www.syntonize.com. https://www.syntonize.com/que-es-el-darkverse-una-nueva-amenaza/