BARATARIA
Revista Castellano-Manchega de Ciencias Sociales
Nº 35, pp. 1-14, 2024, ISSN: 1575-0825, e-ISSN: 2172-3184
DOI: https://doi.org/10.20932/barataria.v0i35.683

METAVERSO Y SEGURIDAD INTERNACIONAL. RIESGOS Y POTENCIALES AMENAZAS

METAVERSE AND INTERNATIONAL SECURITY. RISKS AND POSSIBLE THREATS

José Miguel Calvillo Cisneros
Universidad Complutense de Madrid / España
jcalvill@ucm.es
https://orcid.org/0000-0003-3340-184X

Recibido/Received: 5/03/2024
Modificado/Modified: 6/5/2024
Aceptado/Accepted: 18/5/2024

RESUMEN
El desarrollo de la Inteligencia Artificial afecta a las formas de concebir la seguridad nacional e internacional de nuestro tiempo. Nuevas herramientas de control y defensa, pero también desafíos que surgen en un espacio virtual difícilmente controlable por los Estados y las organizaciones internacionales. En este paradigma surge el metaverso como espacio virtual anárquico, donde se desarrollan actividades recreativas, originales formas de consumo y de marketing, pero también acciones violentas y de desestabilización nunca vistas anteriormente. Estos hechos han derivado en un aumento de la participación de actores no estatales en parcelas tradicionalmente competencia de los Estados. También ha aumentado la actividad de organizaciones del crimen organizado y de grupos terroristas. Por otro lado, que los Estados usen estas tecnologías implica riesgos en materia de derechos humanos y libertades civiles. Existe una necesidad imperiosa de establecer marcos de gobernanza internacional que ayuden a prevenir conflictos y promover el uso responsable de estas tecnologías.

PALABRAS CLAVE
Metaverso, inteligencia artificial, seguridad internacional, ciberseguridad, revolución 4.0.

SUMARIO
1. Introducción. 2. La seguridad y su relación con el espacio tecnológico. 3. Principales amenazadas en el interior del metaverso. 4. Metaverso, terrorismo y crimen organizado. 5. Conclusiones. Bibliografía.

ABSTRACT
Artificial Intelligence affects the way we understand national and international security. New tools for control and defense, but also new challenges that appear within a virtual world that is difficult for States and International Organizations to control. In this new paradigm, the Metaverse appears as a virtual and anarchic space, where recreational activities, new ways of consuming and trading, and violent and destabilizing actions never seen in the past take place. As a result, the involvement of non-state actors, in areas traditionally under the authority of states, has increased, and terrorist and illicit activities in cyberspace have grown. Moreover, if states use this technology, it poses some risk to human rights and

freedom. We must create an international governance framework to prevent conflict and promote responsible use of Artificial Intelligence and the metaverse.

KEYWORDS
Metaverse, Artificial Intelligence, International Security, Cybersecurity, Revolution 4.0.

CONTENTS

1. INTRODUCCIÓN

Las amenazas a la seguridad internacional persistentemente están evolucionando y adaptándose a las tecnologías que han ido surgiendo a lo largo de la historia. La aparición del arma nuclear, por ejemplo, supuso un cambio mayúsculo en la concepción de una amenaza real de desaparición de la especie humana lo que conllevó una serie de cambios políticos y normativos que afectaron al comportamiento de los Estados. Similar fue el uso de las armas químicas durante la Primera Guerra Mundial que fue un punto de inflexión en la forma de concebir la guerra.

En la actual era digital, la seguridad internacional se encuentra inmersa en los desafíos derivados de la cuarta revolución tecnológica -Revolución 4.0-. En este sentido, la evolución de la Inteligencia Artificial (IA) está transformando la forma en que las naciones interactúan y se relacionan poniéndose de manifiesto los riesgos y beneficios significativos para la seguridad a nivel global. Por un lado, esta revolución tecnológica abre un abanico de nuevas herramientas de la seguridad del control, defensa y ataque contra amenazas difícilmente identificadas, pero, por otro lado, también se vislumbran nuevos desafíos difíciles de enfrentar con instrumentos clásicos como son la desinformación a través de Internet y las redes sociales y la consiguiente manipulación de la opinión pública, los procesos de radicalización o los ciberataques. La IA en su conjunto tiene la capacidad de procesar una gran cantidad de datos y, tras su tratamiento, tomar decisiones con un impacto significativo en cuestiones relacionadas con la seguridad. Por ejemplo, la Unión Europea en su política de control fronterizo está utilizando modelos probabilísticos de IA para controlar, detectar embarcaciones e incluso para tomar decisiones que afectan a la seguridad en el Mediterráneo.

La industria de la defensa ha adaptado las nuevas herramientas de IA al campo de la seguridad internacional transformando el diseño del armamento, pero también las estrategias comunicativas y de información (García-Río, et al, 2022). De alguna forma, son conscientes de que "la producción de información útil orientada a la toma de decisiones en seguridad nacional no podrá mantenerse aislado, en los próximos años, del impacto por la revolución tecnológica, que afecta a todos los estratos de la sociedad humana" (Pérez, 2019, p. 3).

La IA se está usando para la creación de nuevas formas de transporte terrestre, marítimo y aéreo que desempeñan funciones de reconocimiento, vigilancia, rescate e, incluso, combate; es utilizada para analizar grandes cantidades de datos, imágenes, grabaciones de audio y video, y otras fuentes de información para identificar patrones, amenazas y objetivos agilizando la toma de decisiones y la capacidad de respuesta ante una situación de alta peligrosidad; es un instrumento esencial para detectar y prevenir ciberataques identificando patrones de comportamiento y detectando posibles amenazas digitales (Singer y Friedman, 2014); puede optimizar la gestión de la cadena de suministro militar, pronosticar necesidades de

mantenimiento y reparación de equipos; facilita la toma de decisiones autónomas en tiempo real por parte de sistemas militares, como vehículos no tripulados y sistemas de armas autónomas, con los debates éticos que plantea. Por otro lado, no es nada desdeñable, la capacidad de tomar decisiones de forma autónoma y con una rapidez nunca vista hasta nuestro tiempo; la IA también tiene un impacto significativo en la industria de la simulación y entrenamiento creando entornos de simulación avanzados para el entrenamiento de soldados y pilotos. A través del metaverso (Ball, 2022), estos sistemas podrán simular situaciones de combate realistas y adaptarse a las acciones de los participantes. Parece ya evidente que "La inteligencia basada exclusivamente en la cognición humana se está convirtiendo en algo demasiado costoso y, en cierto modo, anacrónico. La prospectiva, basada exclusivamente en el juicio de un "experto" tiene los días contados" (Pérez, 2019, p. 4).

El objetivo central de este artículo es identificar las principales amenazas a la seguridad, nacional e internacional, a través del uso de la IA en general, y del metaverso en particular. Para ello, analizamos los nuevos patrones de comportamiento en el campo de la seguridad internacional estudiando las potenciales ventajas y desventajas que se derivan de su uso. Las variables que analizamos son los riesgos provenientes del uso de la IA y del metaverso por actores no estatales, como organizaciones del crimen organizado y grupos terroristas. Cabe advertir que los temas relacionados con la seguridad internacional, la defensa y la IA y los espacios virtuales de simulación plantean un abanico de preocupaciones éticas (Etzioni y Etzioni, 2017; González y Martínez-Cardero, 2020) sobre su uso como son el tratamiento de los datos o la privacidad de las personas. En definitiva, la IA tiene un impacto profundo en la industria de la defensa al mejorar la eficiencia operativa, la precisión en la toma de decisiones y la capacidad de respuesta. Sin embargo, su uso plantea desafíos éticos y de seguridad que deben ser abordados de manera cuidadosa y responsable. Asimismo, al adentrarnos en un mundo aún incipiente y que actualmente solo forma parte de los laboratorios cibernéticos nos conduce a un escenario excesivamente interpretativo. Por último, cabe advertir que estamos dentro de un área de estudio donde convergen diferentes disciplinas académicas como las matemáticas, la ingeniería, la estadística, la computación, la psicología, las ciencias políticas, las relaciones internacionales, etc. Nuestro marco conceptual y epistemológico se enmarca en las dos últimas, las disciplinas de las Relaciones Internacionales y de la Ciencias Políticas, a sabiendas de que la IA y sus derivadas como el metaverso nacen y se desarrollan en el seno de áreas del conocimiento alejadas de los estudios internacionalistas y politológicos.

2. LA SEGURIDAD Y SU RELACIÓN CON EL ESPACIO TECNOLÓGICO

La seguridad internacional en la actualidad se explica a través del análisis de una multitud de variables que son imprescindibles para detectar las principales amenazas y desafíos a los que se enfrenta la humanidad de nuestro tiempo (Calvillo, 2022). Este contexto de policrisis (Sanahuja, 2023) o crisis superpuestas combina factores como el cambio climático, la polarización política y social, la inflación, la crisis de las materias primas y las tensiones geoeconómicas con consecuencias impredecibles (Rivera, 2023), y a todas estas causas habría que añadir los efectos negativos que tienen los avances tecnológicos en la desestabilización social. La seguridad internacional ha adquirido, por tanto, una complejidad sin precedentes, sobre todo desde que nos encontramos inmersos en la era digital donde la ciberseguridad y la IA desempeñan un papel protagonista (Richards, 2014; Schmidt, 2022). En este marco de análisis, el metaverso emerge como un concepto novedoso que vislumbra cambios en el comportamiento social de los actores que conviven en nuestra comunidad global afectando,

aun de manera todavía incierta, a la seguridad internacional. La ciberseguridad, la IA, el *big data* (Cukier y Mayer-Schoenberger, 2013), el metaverso…, son elementos esenciales para poder comprender los cambios que nos dirige a un nuevo paradigma de la seguridad internacional, en el cual se empieza a entrever alteraciones en los elementos primarios o sustanciales que configuran a los Estados-nación como es, por ejemplo, una pérdida parcial de la soberanía para asuntos referidos a la seguridad.

Tradicionalmente, los Estados han monopolizado las cuestiones relacionadas con la seguridad nacional e internacional. Hasta no hace muchos años, las amenazas se contemplaban por la posibilidad de que otro Estado pudiera atacar con el fin de ganar o recuperar territorio, imponer su visión del mundo, conseguir mayor cuota de poder, etc. Recientemente, sobre todo desde los atentados del 11 de septiembre de 2001, se ha ampliado el abanico de riesgos contra la soberanía de los Estados incluyendo a los grupos terroristas, organizaciones del crimen organizado y, ya asumido universalmente, nuevas amenazas que provienen del deterioro medioambiental, la pobreza extrema y las pandemias. La seguridad, como las sociedades, se encuentra en un constante cambio y las amenazas a su estabilidad se han diversificado dejando de ser monopolio exclusivo de los Estados.

Existe consenso entre académicos y profesionales de que la evolución tecnológica está transformando los asuntos relacionados con la seguridad nacional e internacional (Fuertes, 2022). El informe de la Comisión de Seguridad Nacional de los Estados Unidos (NSCAI) de 2021 afirma que: "la capacidad de una máquina para percibir, evaluar y actuar con mayor rapidez y precisión que un ser humano representa una ventaja competitiva en cualquier campo, civil o militar. Las tecnologías de IA serán una fuente de enorme poder para las empresas y los países que las aprovechen" (2021, párr. 5). Tanto el control, como el uso de las herramientas de IA y de los espacios virtuales equivale a tener una mayor capacidad para influir en el espacio y en el comportamiento del resto de actores internacionales y, de alguna manera, determinar patrones de conducta. Aunque debemos de ser conscientes de que la actividad en estos espacios virtuales también puede generar reacciones contestatarias de actores *outsiders* del sistema.

En este sentido, es necesario aclarar que el ciberespacio carece de soberanía. Esta afirmación fue sostenida por John Perry Barlow en el Foro de Davos de 1996 cuando subrayó que: "Gobiernos del Mundo Industrial, vosotros, cansados gigantes de carne y acero, vengo del ciberespacio, el nuevo hogar de la mente. En nombre del futuro, os pido que nos dejéis en paz en el pasado. No sois bienvenidos entre nosotros. No ejercéis ninguna soberanía sobre el lugar donde nos reunimos" (Quintana, 2016, p. 12). Los Estados más poderosos, conscientes del riesgo que supone un descontrol de este espacio, tratan de ejercer su control e influencia en el ciberespacio. De hecho, una de las evidencias que supone las revelaciones de Edward Snowden es, precisamente, el control digital que ejercen las fuerzas de seguridad, en este caso de los Estados Unidos, de este entorno digital.

La revolución tecnológica 4.0 es, además, un espacio de confrontación entre las potencias hegemónicas mundiales, en especial Estados Unidos y la República Popular de China (en adelante China), que libran una batalla por liderar el mercado de los semiconductores, la IA y todo lo relacionado con la industria cibernética. En esta línea, por ejemplo, "la Administración Biden anunció nuevas sanciones en octubre de 2022 y una nueva ley, las *Chips Act*, que prohíbe a cualquier compañía de tecnología de semiconductores que reciba dinero público invertir en instalaciones ubicadas en China. El objetivo es detener los progresos del gigante asiático con la IA" (Miller, 2023, p. 22). Estamos inmersos en lo que se ha denominado la *cuarta revolución industrial* que se caracteriza por la confluencia simultánea de numerosas tecnologías exponenciales como el *big data*, la IA, el *blockchain*, la computación cuántica, la robótica, la realidad virtual, la ciberseguridad y biometría, la nanotecnología, la biotécnica, la impresión

3D, el *Building Information Modeling* (BIM), los vehículos autónomos y los drones, entre otras (Serrano, 2022). Una nueva vuelta de tuerca en una cuarta revolución tecnológica que afecta a todas las parcelas de la vida, incluida la seguridad.

Una diferencia importante entre lo que sucede en el ciberespacio y en el metaverso es que en el primero los ataques tienen consecuencias reales, un impacto medible en las vidas humanas, mientras que las actividades que se desarrollan en un entorno virtual, en principio, no van más allá y sus consecuencias en el mundo real vienen determinadas por el comportamiento que puedan tener otros actores fuera de él. En este sentido, las implicaciones que el metaverso tiene para la seguridad internacional son inciertas. El metaverso es una herramienta que en el campo de las amenazas internacionales puede servir como teatro de simulación para crear, moldear y eliminar pautas de comportamiento de los individuos que conforman los grupos sociales. Este espacio virtual, de ficción, también puede suponer la construcción de nuevas amenazas y potenciar las existentes.

En este marco, el metaverso puede servir como espacio ideal para introducir mensajes destinados a la manipulación y desinformación que repercuta en la estabilidad y la seguridad de los Estados. Y, también, este espacio virtual puede servir para modificar patrones de conducta, introducir nuevas pautas de comportamiento e incluso ir perfilando nuevas formas de convivencia social que puedan salir del espacio virtual y exportarse a la realidad internacional. A través de las plataformas como el metaverso se pueden difundir discursos, por ejemplo, contra un determinado tipo de inmigración y esto puede calar de forma sencilla en determinados grupos sociales fáciles de adoctrinar (Estay Sepúlveda, 2022). En esta línea, la utilización de imágenes racializadas (Walia, 2022) vinculando a los inmigrantes con actividades criminales y delictivas proyectaría una imagen de odio hacia un grupo poblacional ya de por si altamente vulnerable. Esta circunstancia no es nueva, puesto que es frecuente el tratamiento informativo que reciben colectivos criminalizados, como los inmigrantes procedentes del continente africano que se dirigen a Europa o los centroamericanos que desean llegar a los Estados Unidos. Aquí, el metaverso puede proyectar y potenciar narrativas de odio que ya se utilizan en otros formatos (prensa, televisión, redes sociales e Internet fundamentalmente) y reforzar la construcción de una imagen negativa.

A todas luces se vislumbra un cambio de tendencia en cuanto al control que los Estados, como actores dominantes de las relaciones internacionales, ejercen en la parcela de la seguridad. La seguridad nacional e internacional, de ser una competencia inamovible de la sacrosanta soberanía nacional, pasa a formar parte de un escenario alejado de su control donde surgen actores de naturaleza y fines totalmente diferentes que despliegan una influencia destacable y que repercute en la estabilidad de las sociedades. En este sentido, las relaciones entre la industria de la tecnología y los departamentos de seguridad y defensa en, por ejemplo, los Estados Unidos, ha sido una constante desde la Segunda Guerra Mundial (Miller, 2023), pero en las últimas décadas se ha producido una relación de dependencia casi absoluta. El trabajo elaborado por Christopher R. Moran, Joe Burton y George Christou afirma que: "los Departamentos de Seguridad y defensa han reconocido desde hace mucho tiempo la necesidad de colaborar con el sector tecnológico en el campo de la IA. Sin embargo, estas relaciones conllevan ciertos desafíos ya que el sector es una curiosa amalgama de ideologías e intereses diversos" (2023, p.2).

En este espacio aparentemente incontrolado aparece el metaverso, tecnología que con todas sus bondades permiten recrear y avizorar los escenarios del futuro. También se convierte en una plataforma de intercambio de información que puede ser utilizada por grupos ilegales y organizaciones criminales para perpetrar actividades ilícitas (Naim, 2006) que ponen en riesgo la seguridad de la nación (Calderón y Bolaños, 2023). A este fenómeno podemos sumar la

darkweb y *deepweb* cuya característica y capacidad de actuar en el espacio cibernético también está siendo empleada para realizar actividades lícitas como ilícitas. Efectivamente, la inexistencia de legislación concreta y de capacidad para controlar un espacio anárquico hace que los Estados sean más vulnerables a comportamientos que se generan y nutren en espacios como el metaverso.

Conviene advertir, en línea con Javier Esteinou Madrid que "este nuevo poder superó la autoridad política ideológica del Estado convencional y se convirtieron en un poder autocrático sin control que influye, presiona, orienta y juzga a todos los grupos sociales, instituciones y sectores, sin que el bien público o el interés común los pueda acotar y dirigir. Paulatinamente dejaron de ser medios y se convirtieron en fines: renunciaron a ser puentes de relación simbólica para edificar la comunicación y se transformaron en eficientísimas herramientas del poder establecido, especialmente privado, para dirigir, controlar y subordinar a los individuos y a los grupos según los proyectos económicos y políticos que los determinan" (2012, p. 132). Esto viene a confirmar, en palabras de Beatriz Treviño que "la tecnología y su acceso global ha configurado una nueva forma de relación con la política y con los medios de comunicación, como fuente de poder" (2015, p. 199).

En la Tabla 1 se trata de resumir las principales amenazas a la seguridad provenientes de un tendencioso uso de las herramientas de IA. El control de esta tecnología favorece una posición dominante en el escenario internacional, otorga un protagonismo a la industria tecnológica, no solo desde una perspectiva estrictamente militar, sino también en la construcción de patrones de conducta social y de superioridad económica en el mercado tecnológico. Para que la IA y espacios como el metaverso funcionen se necesitan chips y semiconductores de última generación y en este campo las empresas de Estados Unidos, con fuertes inyecciones de dinero público, ejercen una hegemonía mundial (Miller, 2023). En el otro lado, China trata de reducir la brecha existente (Shattuck, 2021) para desarrollar su propia IA y tener una industria de semiconductores con capacidad de hacer competencia a los Estados Unidos. En esta pugna, el control de Taiwán es esencial puesto que en esta pequeña isla se fabrican aproximadamente dos tercios de los chips y semiconductores del planeta.

Tabla 1: Principales amenazas detectadas a la seguridad provenientes de la IA

Principales amenazas a la seguridad	**Descripción de la amenaza**
Ataques de adversarios	Manipulación de sistemas de IA mediante la introducción de datos maliciosos, virus, etc.
Fugas de datos	Acceso no autorizado a datos sensibles, ya sean de los Estados, como de las personas Pérdida de privacidad
Modelos sesgados	La presencia de sesgos en los datos que puede llevar a resultados sesgados y discriminatorios
Robo de propiedad intelectual	Robo de modelos de IA, algoritmos o datos confidenciales que pueden ser utilizados por otros para beneficio propio o malicioso
Suplantación de identidad	Crear sistemas de IA falsos que pueden imitar la voz o el comportamiento humano para engañar a las personas
Robo de identidad digital	El uso de IA para crear perfiles de usuarios falsos y realizar actividades fraudulentas en línea: *phishing* o la difusión de desinformación
Riesgos en la ciberseguridad	Realización de ataques cibernéticos, como el acceso no autorizado o el *malware* Uso en este espacio de tácticas híbridas o no convencionales

Fuente: Elaboración propia

En definitiva, la cuarta revolución tecnológica -Revolución 4.0- está produciendo cambios sustanciales en la seguridad nacional, tanto en la detención de riesgos a la soberanía, como en el diseño de nuevas estrategias de vigilancia y control, y esto repercute en una nueva forma de entender la seguridad internacional y la geopolítica, pero al mismo tiempo, la Revolución 4.0 está provocando el auge de actores no estatales que se están apropiando de parcelas tradicionalmente parte de la soberanía de los Estados-nación. Este hecho no es particular de esta revolución tecnológica, ni mucho menos. La realidad es que la innovación tecnológica siempre ha precedido a la innovación de los conceptos estratégicos. Pierre Lellouche lo define claramente: "Los estrategas no han inventado la estrategia, sino que, muchas veces, los armamentos dictan la evolución de la estrategia. Esto es válido para la espada, el arco, el cañón, los cohetes intercontinentales, las armas nucleares…" (1987, p. 81).

Efectivamente, tanto la IA, como el metaverso ejercen presión para que los Estados y otros actores internacionales se adapten a una nueva dimensión consecuencia de la evolución tecnológica. En la actualidad, la seguridad cibernética se convierte en una preocupación crítica con el fin de proteger la integridad de los datos, la infraestructura y la información que se mueve en el espacio cibernético y virtual, a sabiendas de que este hecho entra en confrontación directa con algunos pilares básicos de las sociedades liberales como son la libertad individual y la privacidad haciendo válido el clásico dilema entre libertad y seguridad (Sørensen, 2007; Shama, 2023) que se impuso con fuerza, sobre todo, tras los atentados terroristas del 11 de septiembre de 2001.

3. PRINCIPALES AMENAZADAS EN EL INTERIOR DEL METAVERSO

El abanico de amenazas que pueden surgir en el metaverso es variado, aunque todas ellas se generan en un ámbito virtual, no real, pero con altas posibilidades de que terminen condicionando el comportamiento social. Podemos establecer tres ámbitos interrelacionados: el de la información, el del control y el de la regulación (resumen en Tabla 2). En el primero de ellos, el metaverso puede ser utilizado como un espacio para recopilar información sobre amenazas potenciales, tanto internas, como externas, la supervisión de amenazas consideradas sospechosas, la desinformación y la propaganda con implicaciones en la seguridad nacional, la mitigación de campañas que podrían socavar la estabilidad o la confianza pública. La construcción de narrativas e imágenes de odio, mencionadas en el punto anterior, es un ejemplo de cómo a través de un entorno simulado se puede influir en la configuración de una percepción negativa sobre un grupo social determinado, como puede ser la inmigración, la raza, la religión, la pobreza e incluso el sexo.

Uno de los riesgos más prominentes radica en la manipulación de la identidad y la privacidad en este espacio virtual. Dado que los usuarios pueden adoptar avatares y pseudónimos, existe la posibilidad de que individuos malintencionados utilicen esta anonimidad para difundir contenido ofensivo o incitar al odio, lo que podría llevar a la estigmatización y criminalización de ciertos grupos sociales. Otro aspecto preocupante es la creciente dependencia de la realidad virtual en la sociedad, lo que podría dar lugar a la alienación y la desconexión del mundo real. La propaganda dirigida a grupos específicos podría aprovechar esta desconexión para manipular las percepciones y opiniones de los usuarios, exacerbando los prejuicios y promoviendo la polarización (Martín Ramallal y Cárdenas-Rica, 2022; Paredes y Bolaños, 2023). Además, la recopilación masiva de datos en el metaverso plantea riesgos de vigilancia y manipulación que podrían utilizarse en campañas de desprestigio y criminalización. En este contexto, es fundamental que se implementen

medidas de seguridad y regulaciones efectivas para mitigar estas amenazas y garantizar que el metaverso sea un espacio inclusivo y seguro para todos los usuarios.

En relación con el segundo ámbito, el del control, el metaverso podría convertirse en un componente crítico de seguridad de la infraestructura digital de un país. En este sentido, las agencias de seguridad estatales pueden involucrarse en garantizar la disponibilidad y la resiliencia de este tipo de infraestructuras ante posibles desafíos cibernéticos. La prevención de actividades ilícitas y la identificación de amenazas potenciales son esenciales para garantizar una seguridad digital, cada vez más imbricada en la vida pública y privada de las sociedades. También, en la seguridad virtual, el metaverso no tiene fronteras físicas, lo que plantea desafíos en términos de control de acceso y seguridad. Las agencias de seguridad nacional pueden tener un papel en la gestión de la seguridad fronteriza virtual para prevenir la entrada ilegal o actividades ilícitas en el metaverso. El metaverso, además, es un espacio de gran interés para organizaciones terroristas que ven un espacio ideal para llevar a cabo acciones de radicalización.

El metaverso está suscitando inquietudes en relación con la actividad terrorista (Agra, 2022) y las organizaciones del crimen internacional (el siguiente punto de este articulo lo dedicamos a estas cuestiones). Al brindar un grado significativo de anonimato y la capacidad de comunicarse de manera cifrada, el metaverso puede ser aprovechado por grupos terroristas y delictivos para coordinar operaciones, reclutar miembros y difundir su ideología de manera más eficaz y discreta. La naturaleza descentralizada del metaverso dificulta la supervisión y la identificación de estas actividades ilícitas, lo que plantea desafíos significativos para las agencias de seguridad de todo el mundo. Además, la creación y comercio de activos digitales en el metaverso, como criptomonedas no reguladas (Agra, 2022) y bienes virtuales de alto valor, pueden ofrecer una vía para el lavado de dinero y la financiación de actividades criminales y terroristas. Las organizaciones del crimen internacional pueden utilizar el metaverso como un canal para blanquear sus ganancias ilícitas y facilitar transacciones financieras opacas, lo que agrega otra capa de complejidad a los esfuerzos para combatir el crimen transnacional.

Directamente relacionado con los dos puntos anteriores, en el ámbito de la regulación, los Estados han de desempeñar un rol más activo en el desarrollo de marcos regulatorios y políticas públicas dirigidas a controlar la vida dentro del metaverso y poder tener un mínimo de seguridad jurídica. Ahora bien, la velocidad con la que está evolucionando la IA, y todas sus aristas, hace que sea muy complejo crear normas, aunque sean de mínimos, para regular una actividad que se desarrolla en un entorno que no es real, sino virtual. Asimismo, ya que el metaverso es un espacio donde las multinacionales han adquirido una relevancia sobresaliente, ya que es un espacio ideal para la venta de productos y el desarrollo de un marketing dirigido a captar nuevos consumidores, habría que plantearse su participación, activa o pasiva, en la construcción de normas reguladoras.

La Unión Europea ha sido el primer actor a nivel mundial en aprobar una norma sobre la IA. Esta organización internacional propone la construcción de un marco regulador de la IA (Parlamento Europeo, 2024) en función del riesgo que supone su uso y aplicabilidad en los usuarios. En abril de 2021, la Comisión propuso el primer marco regulador de la Unión Europea para la IA: "Propone que los sistemas de IA que puedan utilizarse en distintas aplicaciones se analicen y clasifiquen según el riesgo que supongan para los usuarios. Los distintos niveles de peligro implicarán una mayor o menor regulación. Una vez aprobadas, serán las primeras normas del mundo sobre IA" (Parlamento Europeo, 2024, parr.2). Para la Unión Europea, los sistemas de IA de riesgo inaceptable son los que se consideran una amenaza para las personas y serán prohibidos. Estos son (Parlamento Europeo, 2024, párr. 4):

1. Manipulación cognitiva del comportamiento de personas o grupos vulnerables específicos: por ejemplo, juguetes activados por voz que fomentan comportamientos peligrosos en los niños.
2. Puntuación social: clasificación de personas en función de su comportamiento, estatus socioeconómico o características personales.
3. Sistemas de identificación biométrica en tiempo real y a distancia, como el reconocimiento facial.

La cooperación y colaboración internacional en materia de seguridad cibernética es también un campo esencial para poder abordar las amenazas comunes que representa el metaverso. Para ello, el trabajo conjunto de los cuerpos de policía y de seguridad y defensa es clave para minimizar los riesgos que podrían surgir en este espacio virtual con proyección hacia la realidad.

Tabla 2: Ámbitos de actuación en el Metaverso

Ámbito	Actividad
Información	Recopilar información Luchar contra la desinformación Luchar contra la propaganda
Control	Detectar amenazas potenciales Infraestructuras digitales Prevención de actividades ilícitas Procesos de radicalización y captación
Regulación	Cooperación internacional Marcos regulatorios

Fuente: Elaboración propia

En resumen, el metaverso está emergiendo como un nuevo espacio digital que plantea una serie de desafíos en términos de seguridad nacional e internacional. Las agencias de seguridad y las autoridades gubernamentales están empezando a considerar cómo abordar estos desafíos para garantizar la seguridad y la integridad en este entorno virtual en constante evolución. Lamentablemente, el metaverso, aunque promete un mundo virtual lleno de posibilidades, también presenta amenazas significativas que podrían ser explotadas en la construcción de propaganda dirigida a grupos sociales con la intención de criminalizarlos.

4. METAVERSO, TERRORISMO Y CRIMEN ORGANIZADO

Hasta el momento, no tenemos suficientes evidencias empíricas para establecer una relación directa entre los grupos del crimen organizado, el terrorismo internacional y el uso del metaverso como espacio donde desarrollar actividades ilícitas. No obstante, no es óbice señalar y analizar las hipótesis por las que las organizaciones del crimen y los grupos terroristas pudieran utilizar este espacio virtual para acometer sus acciones violentas en el espacio internacional (Anguita y Gil, 2018), algunas de ellas citadas en el anterior apartado, pero que desarrollaremos en profundidad a continuación.

En primer lugar, el metaverso, como espacio virtual y de ficción, es un área idónea donde los grupos del crimen y del terrorismo pueden reclutar y radicalizar a sus miembros. A través de herramientas de IA se puede localizar a personas vulnerables y susceptibles de ser captadas por este tipo de organizaciones violentas y, a través del metaverso iniciar un proceso de radicalización moldeando su comportamiento y trasmitiendo mensajes de odio que, poco a poco, vayan calando en la construcción de una determinada imagen de un colectivo

identificado como enemigo. Paralelamente, el metaverso también es un espacio donde fidelizar a los miembros de una organización ilícita, incentivando su rol dentro del grupo, valorando su participación e incluso simulando los potenciales beneficios de ser un miembro más activo asumiendo nuevas responsabilidades (Tabla 3).

Evidentemente, el terrorismo existía con anterioridad a Internet y, como es lógico, a la IA, pero, al igual que el resto de los actores sociales, ha sabido adaptarse a las posibilidades que le ofrecen las tecnologías. En esta línea, "la manera de incitar, reclutar, financiar o planificar actos terroristas ha sufrido importantísimos cambios a lo largo de la historia y, uno de los más notorios va de la mano con el crecimiento vertiginoso de instrumentos y estructuras digitales" (Agra, 2022, p. 18). Es cierto que el uso de la tecnología 4.0 añade complejidad a la conceptualización del término terrorismo. Siguiendo a Alice Martini, "el terrorismo es (…) producto de una categorización de un determinado tipo de violencia que tiene lugar en una coyuntura histórica, social y política" (2015, p. 195), lo que nos lleva a la conclusión de que es un concepto en continua evolución y susceptible de los cambios que se producen en la sociedad.

La IA es una herramienta de defensa y de ataque utilizada por los Estados en el espacio cibernético (Quintana, 2016), pero también los grupos terroristas o criminales aprovechan esta tecnología con el fin de perpetrar ataques cibernéticos más sofisticados y difíciles de detectar, como, por ejemplo, la interrupción de servicios críticos o el robo de información sensible. En este sentido, los trabajos realizados por Van Puyvelde y Brantly destacan que:

"States inspire the greatest fear in cyberspace, they are not the most prolific malfeasant actor category or the most pervasive threat to the average netizen. Three other categories of actors, each of which falls under the overarching designation of non-state actor, generate the majority of havoc that occurs in cyberspace. Criminals, hacktivists, and terrorists in combination for exceed states in volume and variety of daily attacks and thefts that occur in and through cyberspace" (2019, p. 105).

Efectivamente, los actores no estatales tienen un protagonismo mayúsculo en el espacio virtual incluso mayor que el de los Estados. La actividad de este tipo de actores ilícitos supera a los Estados en volumen y variedad de ataques y robos diarios que se producen en el ciberespacio (Van Puyvelde y Brantly, 2019). Las escasas y débiles barreras de entrada y el amplio alcance e impacto del ciberespacio permiten a estos actores no estatales generar amenazas a la seguridad de los Estados y, de cierta manera, una violación de su soberanía. Para las organizaciones del crimen y los grupos terroristas la continua expansión del ciberespacio y de sus tecnologías ofrecen un terreno fértil muy amplio para el desarrollo de capacidades dentro de un entorno que plantea pocos riesgos para su seguridad física.

Mientras que el impacto de los ciberataques tradicionalmente se ha centrado en la piratización de páginas web y en el volcado de documentos con información privada, el uso del ciberespacio ha cambiado la forma en que los terroristas se organizan, reclutan y planifican sus operaciones en el mundo físico. De hecho, "en los últimos años, los expertos hacen cada vez más hincapié en el uso del ciberespacio para la organización y planificación de incidentes terroristas" (Van Puyvelde y Brantly, 2019, p. 117). En este marco, el metaverso se presenta como un lugar idóneo en el proceso de captación, entrenamiento y radicalización de los terroristas porque permite crear entornos virtuales donde se puedan diseñar y realizar sesiones de entrenamientos lo más próximo a escenarios reales. De la misma manera, el metaverso también es un espacio donde difundir mensajes, propaganda y actividades de desinformación con la idea de crear contenidos falsos y construir narrativas dirigidas a la radicalización de personas vulnerables y, por tanto, proclives a formar parte de organizaciones del crimen y de grupos terroristas. Además, también es un espacio donde fortalecer liderazgos dentro de los grupos ilícitos.

Tabla 3: Principales amenazas a la seguridad detectadas en el metaverso

Acción	**Objetivos**
Reclutamiento	Captación de nuevos miembros a través de espacios virtuales Fidelización de miembros ya captados
Radicalización	Preparación hacia una fase activa para cometer actos terroristas Potenciación de liderazgos dentro del grupo
Entrenamiento	Simulación de acciones creando espacios similares a situaciones reales
Narrativas	Creación de discursos de odio Identificación de enemigos y de objetivos
Financiación	Blanqueo de capitales Financiación a través del ciberespacio (criptomoneda, criptodivisas…)

Fuente: Elaboración propia

En relación con la financiación ilícita, los entornos virtuales son espacios idóneos para realizar transacciones de grandes cantidades de dinero y no ser detectadas por los organismos internacionales oficiales o los Estados. A través de la IA se pueden elaborar estrategias precisas de lavado de dinero o enmascarar operaciones financieras ilegales. A través de la minería de datos (Bonilla, 2014) se pueden llevar a cabo estrategias de control de activos financieros que se mueven en los entornos más ocultos de la red y que pueden servir para financiar actividades ilícitas y para cometer acciones de terrorismo. El metaverso es un laboratorio de pruebas ideal para observar la efectividad de llevar a cabo estrategias dirigidas al blanqueo de capitales provenientes de actos ilícitos.

Este abanico de amenazas descrito, y que no supone una lista cerrada, supone un serio desafío para la seguridad y, por tanto, obliga a que los actores estatales y las organizaciones internacionales con competencias en la materia realicen esfuerzos en el desarrollo de marcos normativos y de herramientas de IA con el fin de regular, pero también monitorear y prevenir hechos ilícitos en su conjunto. Es importante reiterar que estas son consideraciones teóricas e interpretativas sobre cómo el metaverso y la IA podrían estar relacionados con el terrorismo y el crimen organizado en el futuro. La mayoría de las empresas tecnológicas, los Estados y algunas organizaciones internacionales están trabajando activamente para prevenir el uso indebido de estas tecnologías y garantizar un entorno, real y virtual, más seguro.

5. CONCLUSIONES

La relación entre tecnología y seguridad es un clásico en las relaciones internacionales y la Revolución 4.0 no deja de ser un hito más de esta vinculación. Ahora bien, en la evolución de esta tecnología aparecen amenazas a la seguridad no conocidas hasta ahora. De la mano de la IA surgen un abanico amplio de herramientas de control, defensa y ataque contra amenazas difícilmente identificadas, pero paralelamente, brotan nuevos desafíos difíciles de enfrentar con instrumentos clásicos. La manipulación, las amenazas, los discursos de odio contra minorías, la propaganda, la mentira, el engaño, etc., siempre han existido como dinámicas que operan dentro de los grupos sociales, pero el metaverso adquiere una dimensión, tal vez en forma líquida, que lo sitúa en un plano aparentemente incontrolado por los Estados. Este hecho ha provocado que la industria de la defensa esté adaptando las nuevas herramientas de IA al

campo de la seguridad internacional lo que conlleva una transformación en el diseño del armamento, los entrenamientos, las estrategias comunicativas y la obtención de información.

El objetivo de este trabajo era identificar las principales amenazas a la seguridad, nacional e internacional, a través del uso de la IA en general, y del metaverso en particular. En primer lugar, las potenciales amenazas detectadas por el uso de la IA han sido la manipulación e intromisión en espacios Web a través de cualquier tipo de virus, troyanos, etc.; la obtención de datos sensibles de Estados, empresas y/o individuos, lo que supone una pérdida de privacidad sin precedentes; el robo de propiedad intelectual; la suplantación de identidad a través de programas que imitan la voz y la imagen de otros seres humanos; la difusión de información falsa con una proyección global en tiempo real; y los ciberataques y el ciberterrorismo utilizado por organizaciones del crimen internacional y grupos terroristas. Estas amenazas detectadas no suponen una lista estanca, sino que se irá ampliando conforme se vaya avanzando en el uso de la IA.

En segundo lugar, los desafíos procedentes del metaverso son más complejos e hipotéticos dado que su implementación es todavía una idea. En el metaverso como espacio virtual se pueden desarrollar actividades de reclutamiento, radicalización, entrenamiento y capacitación, construcción de narrativas manipuladas y vías de obtención de financiación a través de mercados ilícitos. Ciertamente, un metaverso incontrolado por los Estados y organizaciones internacionales puede ser un espacio idóneo para la captación y fidelización de personas susceptibles de formar parte de organizaciones del crimen internacional y de grupos terroristas, como, por ejemplo, la captación de lobos solitarios como versos sueltos en la comisión de ataques terroristas. Este espacio virtual se convierte en un entorno de simulación incontrolado para poder transmitir mensajes de odio, fijar objetivos, en principio simulados, e identificar como nuestros enemigos a grupos sociales, individuos, gobiernos, empresas, etc.

En la actualidad, más que nunca, existe una relación directa entre Estados y actores no estatales en aras de garantizar entornos, reales y virtuales, más seguros. La IA es el cemento, pero también el disolvente de esta vinculación ya que proporciona, de un lado, las herramientas idóneas para avanzar hacia sistemas de control, seguridad y defensa evolucionados, pero, de otro lado, surgen nuevos desafíos difícilmente controlables por los Estados y organizaciones internacionales.

Concluimos que gracias a la IA y el impulso que ejerza el metaverso, se transformarán los entornos de seguridad y supondrá, cada vez más, la participación de actores no estatales con objetivos y naturaleza diferentes. Además, se producirá un crecimiento exponencial de los ciberataques y del ciberterrorismo lo que conllevará que los Estados utilicen herramientas de IA para detectar y eliminar amenazas a su soberanía. Otra de las cuestiones es que los Estados pueden utilizar estas tecnologías para el espionaje y el control, lo que tiene implicaciones importantes en materia de derechos humanos y libertades civiles.

Finalmente, la relación entre Estados, IA y el metaverso en el campo de la seguridad internacional es una cuestión de creciente relevancia en un mundo cada vez más digitalizado y globalizado, aunque es una relación compleja y en constante evolución, lo que dificulta su regulación. A medida que estas tecnologías avancen será fundamental abordar en profundidad las cuestiones que afecten a la seguridad, privacidad, gobernanza y regulación para garantizar un entorno global más seguro y estable. Aunque no se pueden poner puertas al campo, en el marco de la seguridad y la IA existe una necesidad imperiosa de establecer marcos de gobernanza internacional que ayuden a prevenir conflictos y promover el uso responsable de estas tecnologías.

BIBLIOGRAFÍA

Anguita Olmedo, C. y Gil, J. M. (2018). El crimen organizado en la era digital: (re) adaptación a la crisis de la Covid-19. En J.C. Figuereo-Benítez y R. Mancinas-Chávez. *Las redes de la comunicación. Estudios multidisciplinares actuales* (pp. 38-64). Dykinson.

Ball, M. (2022). *El Metaverso. Y como lo revolucionará todo.* Ediciones Deusto.

Bartolomé, M. (2019). Amenazas y conflictos híbridos: características distintivas, evolución en el tiempo y manifestaciones preponderantes. *Revista URVIO* (25), 8-23. https://doi.org/10.17141/urvio.25.2019.4249

Bernal Treviño, A. I. (2015). Tecnología, redes sociales, política y periodismo. ¿Pluralidad informativa o efecto bumerán? *Cuadernos de Información* (36), 191-205. http://dx.doi.org/10.7764/cdi.36.647

Bonilla Murillo, L. (2014). IA Aplicada en la Prevención y Detención de Lavado de Activos y Financiamiento del Terrorismo. *BAC-Credomatic Network*, 1-34.

Calvillo Cisneros, J. M. (2022). Seguridad y Desarrollo. La interrelación de dos políticas públicas en la Agenda 2030. En Pastor Albadalejo, G. y Sánchez Medero, G., *Políticas Públicas en el marco de la Agenda 2030* (pp. 261-286). Tirant lo blanch.

Cukier, K. y Mayer-Schoenberger, V. (2013). The rise of Big Data. Foreign Affairs, 28-40.

Estay Sepúlveda, J. G. (2022). Democracia y Medios de Comunicación en línea: una nueva forma de discurso de odio con la IA como telón de fondo. *Revista de Filosofía*, 39(100), 63-77. https://doi.org/10.5281/zenodo.5979731

Esteinou Madrid, J. (2012). Los medios electrónicos de difusión masiva y la crisis de la cultura en México. *Argumentos* (68), 131-132.

Etzioni, A. y Etzioni, O. (2017). Incorporating Ethics into Artificial Intelligence. *The Journal of Ethics* (21), 403-418. https://doi.org/10.1007/s10892-017-9252-2

Francisco Agra, S. V. (2022). La Digitalización del miedo: del terrorismo "clásico" al terrorismo "tecnológico". *El Criminalista digital. Papeles de Criminología* II Época, 17-37.

Friedman, P. W. (2014). *Cybersecurity and Cyberwar.* Oxford University Press.

Fuertes, M. (2022). *Metamorfosis del Estado. Maremoto digital y ciberseguridad*. Marcial Pons.

García-Rico, E., Baena-Luna, P., Palos-Sánchez, P. R. y Aguayo-Camacho, M. (2022). Amenazas de los gobiernos electrónicos: el desafío de la e-seguridad. *Revista de Pensamiento Estratégico y Seguridad* (CISDE), 7(2), 87-107

González Arencibia, M. y Martínez Cardero, M. (2020). Dilemas éticos en el escenario de la IA. *Economía y Sociedad*, 25(57), 1-17. https://doi.org/10.15359/eys.25-57.5

Lellouche, P. (1987). Influencia de las nuevas tecnologías sobre las concepciones estratégicas actuales. En M. Castells. *Impacto de las tecnologías avanzadas sobre el concepto de seguridad* (pp. 81-94). FEPRI.

Martín Ramalla, P. y Cárdenas-Rica, M. L. (2022). Metaverso como ciberfuente para el periodismo político. *Revista Prisma Social* (39), 95-123.

Martini, A. (2015). Terrorismo: un enfoque crítico. *Relaciones Internacionales*, 28, 191-199.

Miller, C. (2023). *La guerra de los chips. La gran lucha por el dominio mundial.* Península.

Moran, C. R., Burton, J. y Christou, G. (2023). The US Intelligence Community, Global Security, and AI: From Secret Intelligence to Smart Spying. *Journal of Global Security Studies*, 8(2), 1-18. https://doi.org/10.1093/jogss/ogad005

Naim, M. (2006). *Ilícito. Como el contrabando, los narcotraficantes y la piratería desafían la economía global*. Editorial Debate.

NSCAI (2021). *Final Report Artificial Intelligence.* National Security Commission on Artificial Intelligence, https://www.nscai.gov/wp-content/uploads/2021/03/Full-Report-Digital-1.pdf

Paredes, D. M. y Bolaños, E. (2023). El Metaverso y las nuevas amenazas a la seguridad del Estado. *Revista Academia de Guerra del Ejército Ecuatoriano*, 16(1), 122-133. https://dx.doi.org/10.24133/RCSD.VOL16.N01.2023.09

Parlamento Europeo (2024). Ley de IA de la UE: primera normativa sobre IA. *Temas del Parlamento Europeo*. 13/03/2024. https://www.europarl.europa.eu/news/es/headlines/society/20230601STO93804/ley-de-ia-de-la-ue-

primera-normativa-sobre-inteligencia-artificial
Pérez, F. A. (2019). *El enfoque probabilístico en Inteligencia Artificial*. Grupo de Estudios en Seguridad Internacional (GESI). Universidad de Granada, 1-12.
Quintana, Y. (2016). *Ciberguerra.* La Catarata.
Richards, J. (2014). *Cyber-War. The anatomy of the Global Security Threat.* Palgrave Macmillan.
Rivera Albarracín, L. (2023). Crisis climática: retos y oportunidades. *Anuario CEIPAZ 2022-2023*, 59-75.
Sanahuja Perales, J. A. (2023). La Unión Europea y la guerra de Ucrania: dilemas de la autonomía estratégica y la transición verde en un orden mundial en cambio. *Anuario CEIPAZ 2022-2023*. Centro de Investigación y Estudio de la Paz (Ceipaz), 23-58.
Schmidt, E. (2022). AI, Great Power Competition & National Security. *Daedalus* 151(2), 288-298. https://doi.org/10.1162/daed_a_01916
Serrano Acitores, A. (2022). *Metaverso y derecho.* Tecnos.
Shama, A. (2023). Blurred lines: the convergence of military and civilian uses of AI & data use and its impact on liberal democracy. *Política Internacional*,60(4), 879 - 889. https://doi.org/10.1057/s41311-021-00351-y
Shattuck, T. J. (2021). Stuck in the Middle: Taiwan's Semiconductor Industry, the U.S.-China Tech Fight, and Cross-Strait Stability. *Foreign Policy Research Institute*, 101-117. https://doi.org/10.1016/j.orbis.2020.11.005
Sørensen, G. (2007). After the Security Dilemma: The Challenges of Insecurity in Weak States and the Dilemma of Liberal Values. *Security Dialogue*, 38(3), 357-378.
Van Puyvelde, D. y Brantly, A.F. (2019). *Cybersecurity. Politics, Governance and Conflict in Cyberspace*. Polity Press.
Walia, H. (2022). *Frontera y Ley. migración mundial, capitalismo y el auge del nacionalismo racista.* Rayo Verde.

Breve currículo:

José Miguel Calvillo Cisneros
Profesor Contratado Doctor de Relaciones Internacionales en el Departamento de Relaciones Internacionales e Historia Global de la Universidad Complutense de Madrid (UCM). Doctor en Relaciones Internacionales por la UCM desde 2010. Es codirector del Grupo de Investigación: Seguridad, Desarrollo y Comunicación en la Sociedad Internacional en la UCM. Sus líneas de investigación son: los vínculos de la seguridad y el desarrollo, las migraciones forzadas, la seguridad internacional, la cooperación internacional y la acción humanitaria. Dedica especial atención a estudio de Afganistán.

Agradecimientos:
Este artículo es el resultado de las investigaciones realizadas en el Instituto Portugués de Relaciones Internacionales (IPRI) de la Universidad NOVA de Lisboa en el marco de una estancia de investigación durante el curso académico 2023/24. Igualmente indicar que el trabajo está vinculado al proyecto de investigación: *Conflictos armados y crisis humanitarias. Las humanidades y ciencias sociales ante los desafíos de la seguridad multidimensional* (IRENETIKA).