Documento
Opinión

40/2023 24 de abril de 2023

Ana María Martín Elvira

El metaverso: potenciales riesgos y amenazas para la paz y la seguridad, y su contagio en el mundo real

El metaverso: potenciales riesgos y amenazas para la paz y la seguridad, y su contagio en el mundo real

Resumen:

El metaverso nos ofrece un nuevo entorno virtual en el que desarrollar nuestra vida cotidiana. Como parte de esta vida, también abarca todos aquellos aspectos relacionados con nuestra seguridad y defensa, incluyendo los riesgos y amenazas que ponen en peligro nuestra paz y seguridad ante la posibilidad de un contagio de estos al mundo real.

Palabras clave:

Metaverso, ciberespacio, seguridad, paz y contagio.

Ana María Martín Elvira

The metaverse: potential risks and threats to peace and security and their spillover to the real world

Abstract:

The metaverse offers us a new virtual environment in which to develop our daily life. As part of this life, it also includes all those aspects related to our security and defense, including the risks and threats that endanger our peace and security in the possibility of a spillover of these to the real world.

Keywords:

Metaverse, cyberspace, security, peace, spillover.

Cómo citar este documento:

MARTÍN ELVIRA, Ana María. *El metaverso: potenciales riesgos y amenazas para la paz y la seguridad y su contagio en el mundo real*. Documento de Opinión IEEE 40/2023. https://www.ieee.es/Galerias/fichero/docs_opinion/2023/DIEEEO40_2023_ANAMAR_Metaverso.pdf y/o enlace bie[3] (consultado día/mes/año)

Introducción

En 1992, el autor estadounidense de ciencia ficción Neal Stephenson publicó la novela *Snow Crash*, en la que aparecía el metaverso y se definía por primera vez en la historia como un mundo virtual, accesible desde Internet, en el que las personas podían interactuar entre sí y con objetos dentro de un entorno inmersivo compartido[1]. Desde entonces, el concepto de metaverso no solo ha evolucionado con el tiempo, llegando a definirse de diferentes maneras, sino que también ha llegado a materializarse y a ampliar los límites más allá de lo que Neal Stephenson presentaba en su novela, llegando a tener implicaciones en el mundo real.

El concepto y las definiciones del metaverso han evolucionado desde su primera aparición en 1992 en paralelo al avance de la tecnología y sus aplicaciones. En la actualidad, el metaverso se entiende como «un futuro entorno virtual persistente e interconectado en el que los elementos sociales y económicos reflejan la realidad»[2]. Aunque esta definición, que también tiene en cuenta las capacidades de los usuarios y las posibilidades de avance que ofrece el metaverso, incluye todos los aspectos relevantes para una primera comprensión de lo que supone el metaverso, la rápida expansión tanto de las tecnologías como de este nuevo entorno virtual imponen limitaciones a la hora de generar una única definición general para todos los ámbitos.

En su breve trayectoria, el metaverso ha sido definido de diferentes maneras por distintos sectores, pero manteniendo siempre una característica común: su fuerte relación con el sector tecnológico y el entorno virtual. Esta característica es la que no debemos dejar de lado, de hecho, se puede encontrar reflejada en el desarrollo del concepto tanto en libros, películas, videojuegos o incluso en avances tecnológicos como la realidad virtual o la realidad mixta, donde la convergencia entre el mundo real y el mundo tecnológico está presente[3].

Actualmente, podemos observar cómo la palabra metaverso ha sido invocada en diversos contextos, adoptando incluso en su definición los objetivos y motivaciones de

[1] STEPHENSON, Neal. *Snow crash*. Penguin, Harmondsworth, 1993. ISBN 0140230211.
[2] WORLD ECONOMIC FORUM. «Defining and Building the Metaverse», *World Economic Forum* [en línea]. 2021. Disponible en: https://initiatives.weforum.org/defining-and-building-the-metaverse/home [consulta: 15/2/2023].
[3] BAZIN, Aaron. «The Metaverse: A New Domain of Warfare? », *Small Wars Journal* [en línea]. 2022. Disponible en: https://smallwarsjournal.com/jrnl/art/metaverse-new-domain-warfare [consulta: 15/2/2023].

organizaciones internacionales, como la Unión Europea, o empresas privadas como Meta. Esto, como se ha expresado anteriormente, dificulta el desarrollo de una definición única, así como la identificación de las características centrales y la distinción entre las tecnologías relacionadas que soportan el metaverso.

De esta manera, se tomará como referencia la definición de metaverso ofrecida por Styllanos Mystakidis en su artículo «Metaverse», siendo definido como «el universo de la posrealidad, un entorno multiusuario de persistencia perpetua que fusiona la realidad física con la virtualidad digital»[4]. Esta definición permite adaptar el concepto básico a las características y experiencias de cada campo, lo que permitirá en este trabajo, acomodar el concepto al campo de la seguridad y defensa, específicamente aplicado a la paz y la seguridad.

El metaverso y la seguridad y la defensa

A pesar de la ausencia de una definición del metaverso aplicada al ámbito de la seguridad y la defensa, la definición básica ofrecida por Styllanos Mystakidis permite establecer un punto de partida para el sector. Asimismo, la estrecha relación entre el metaverso y el ciberespacio nos permite identificar inicialmente su potencial en el campo de la seguridad y la defensa.

Como se ha indicado anteriormente, cuando hablamos del metaverso, nos referimos al espacio virtual y multiusuario que existe en el entorno digital y que converge con el entorno real. Por otro lado, el ciberespacio se entiende como una red de dispositivos digitales y ordenadores interconectados entre sí, creando una red y un entorno virtual asociado a ella.

Aunque inicialmente puedan percibirse como entornos diferentes, en realidad, el metaverso requiere de la existencia del ciberespacio para ser, es decir, el funcionamiento y desarrollo del metaverso está ligado al ciberespacio, siendo este el entorno o red interconectada en la que se *aloja*. Recíprocamente, la existencia del metaverso

[4] MYSTAKIDIS, Stylianos. «Metaverse», *Encyclopedia* [online], vol. 2, no. 1. 10 February 2022, pp. 486-497. DOI 10.3390/encyclopedia2010031. Available from: http://dx.doi.org/10.3390/encyclopedia2010031 [consulta: 22/2/2023].

proporciona ventajas al ciberespacio a través de la creación de oportunidades para los ciberataques o la ciberdelincuencia, entre otras.

Así, a la hora de desarrollar una definición del metaverso en relación con la seguridad y la defensa, debemos tener en cuenta la relación entre el ciberespacio y este ámbito, ya que todo lo que existe en la red puede transferirse al espacio metaverso. Esta transferencia no solo incluiría aquellos elementos beneficiosos como los marcos regulatorios o la ciberseguridad, sino también la otra cara de la moneda y problemas como la ciberdelincuencia, los ciberataques o el ciberespionaje, entre otros, que ponen en riesgo nuestra paz y seguridad y aumentan aún más las posibilidades de un contagio en el mundo real como se ha observado con los casos del ciberespacio.

Como vemos, aunque no directamente, el entorno general en el que se engloba el metaverso ya tiene una fuerte vinculación con la seguridad y la defensa. En el caso del metaverso, el uso del ciberespacio en el ámbito de la seguridad y la defensa estaría relacionado con este entorno virtual y de las tecnologías asociadas al ciberespacio en operaciones militares y otras cuestiones de seguridad actuales. Sin olvidar que este mismo espacio puede ser utilizado para la guerra u otras actividades disruptivas e ilegítimas, el metaverso puede ofrecer la posibilidad de entrenar personal militar, almacenar información y obtener inteligencia, así como transferir información de forma más eficaz y rápida que de la forma tradicional.

También ofrece la posibilidad de establecer un marco de cooperación más amplio que el habitual, pudiendo abarcar espacios virtuales que actualmente están limitados a marcos normativos. Asimismo, este espacio plantea nuevos retos en la protección de activos militares, así como nuevas oportunidades para la ciberdefensa y los ataques en este campo.

En conclusión, podemos ver cómo, a pesar de la ausencia de una definición fija y de casos de referencia, la relación existente entre el ciberespacio y el ámbito de la defensa y la seguridad sienta las bases del metaverso, un espacio que aporta nuevas dimensiones a los retos y oportunidades del ciberespacio.

El metaverso y la paz y la seguridad

Identificación de los riesgos potenciales para la paz y la seguridad en el metaverso

A la hora de analizar los principales riesgos y amenazas para la paz y la seguridad en el metaverso, una de las principales ideas que debemos tener en cuenta es que la mayoría de los problemas identificados en este entorno virtual son los derivados de la experiencia y casos vividos en el ciberespacio. A continuación, detallaremos aquellos más relevantes para el metaverso, teniendo en cuenta la capacidad de evolución, a corto y largo plazo, de los mismos en este nuevo entorno, así como los diferentes aspectos que abarcan, desde el desarrollo de comunidades extremistas hasta la proliferación de la actividad virtual de las mismas en nuestro entorno real.

Al igual que en el ciberespacio, el metaverso ofrece un nuevo medio y espacio para actividades ilegítimas, proporcionando un marco para el desarrollo e implementación de estas como en el caso del terrorismo o los conflictos. Aunque, hasta la fecha, no existe ningún ejemplo de atentado o conflicto terrorista desarrollado en el metaverso, es cierto que los gobiernos y organismos internacionales se refieren a este nuevo entorno virtual como un nuevo espacio con potencial para el reclutamiento y el desarrollo de actividades terroristas que ofrece nuevas formas de planificar, coordinar, desarrollar y ejecutar actos no legítimos.

Dentro de este marco de actividades ilegítimas, el metaverso también ofrece un espacio para el discurso del odio y el acoso como resultado de la falta de regulación y marcos normativos en torno a estas cuestiones, lo que hace que este espacio virtual no sea inclusivo ni seguro para los usuarios.

Como cualquier otra comunidad *online* y virtual, el metaverso facilita la comunicación y el intercambio de información entre los usuarios, siguiendo un formato similar al del mundo real: a través de su representación en imágenes, vídeos, textos o incluso audios, pero, asimismo, ofrece la posibilidad de crear espacios y nuevas formas de comunicación. En este proceso de comunicación, y como se ha mencionado anteriormente, existe la posibilidad de difundir mensajes de odio, campañas de desinformación, noticias falsas o propaganda, entre otros. En el caso de la propaganda, como identificó Carme Colomina, periodista y profesora, «la propaganda a la vieja

usanza se ha amplificado exponencialmente con la tecnología y la hiperconectividad y su poder y sofisticación se han multiplicado»[5]. En definitiva, esta sentencia expone la idea de cómo los métodos de comunicación tradicionales tal y como los conocíamos se han ido adaptando a los nuevos espacios que han ido surgiendo, y el metaverso es un claro ejemplo de ello.

Como vemos, el metaverso ofrece una nueva posibilidad de comunicación para los grupos extremistas y terroristas, así como un nuevo escenario de reclutamiento. En un estudio realizado por el Centro Nacional de Innovación, Tecnología y Educación Antiterrorista (NCITE, por sus siglas en inglés) en Estados Unidos, los investigadores afirman cómo este entorno virtual facilita el reclutamiento de personas mediante el ejercicio de la coerción y la amenaza, especialmente a través de la difusión de mensajes e ideas asociadas a estas ideologías, permitiendo que aquellas personas con menor capacidad de relación en el mundo real encuentren un refugio y una comunidad en el entorno virtual. Al igual que en los procesos de captación de la última década, principalmente en Internet, las implicaciones para nuestra paz y seguridad son muy elevadas, especialmente si tenemos en cuenta que la posibilidad de que esta actividad se traduzca en un atentado en el mundo real es muy alta, poniendo en riesgo nuestra seguridad.

Además de los riesgos y amenazas identificados, uno de los mayores y más preocupantes para tener en cuenta, y que es objeto de análisis en este trabajo, es la posibilidad de un contagio en el entorno real de las actividades que tienen lugar en el metaverso. En concreto, preocupa la posibilidad de que se produzca un trasvase de ciberataques del entorno virtual al real, convirtiéndose en ciberataques físicos en los que el usuario atacante toma el control, mediante herramientas del metaverso, de sistemas o información del mundo real. Dentro de esta problemática, se debe valorar la suplantación y robo de identidad de otros usuarios como consecuencia de la falta de protección de identidad y datos que existe actualmente en el metaverso, así como la valoración de las capacidades de manipulación y control que se pueden alcanzar a largo plazo como consecuencia de la falta de un marco regulatorio y de protección.

[5] PROSEGUR. «Disinformation, fake news, cyber assaults. How to combat hybrid threats? », *Prosegur* [en línea]. [sin fecha]. Disponible en: https://www.prosegur.com/en/innovation/ciber/disinformation-fake-news-cyber-assaults-how-to-combat-hybrid-threats [consulta: 22/2/2023].

Aunque los riesgos y amenazas expuestos no incluyen todos los que podemos encontrar en el metaverso, sí ofrecen una idea cercana de aquellos que tienen un impacto directo sobre nuestra paz y seguridad, pudiendo explorar otras variantes o implicaciones similares. Cabe señalar que la ausencia de casos prácticos y ejemplos reales de acciones en el metaverso que hayan amenazado nuestra paz y seguridad limita la posibilidad de identificar riesgos cada vez más específicos.

Debate sobre las posibles estrategias para hacer frente a estos riesgos y amenazas

Ante los riesgos y amenazas señalados, los actores, tanto del sector público como del privado, desde el ámbito nacional al internacional, deben tomar medidas para contrarrestar el impacto y hacer frente a los posibles escenarios que puedan poner en peligro nuestra paz y seguridad. Estas medidas, que pueden ir desde el desarrollo de un marco regulatorio a nivel nacional e internacional fruto de la cooperación entre diferentes países y organizaciones internacionales, o el compromiso de intercambiar datos e inteligencia sobre cuestiones relacionadas con estos temas, deben adaptarse a los casos más recientes que existen en el metaverso y, en su defecto, a los que se han vivido en el ciberespacio.

Son varias las razones por las que es necesario tomar decisiones y aplicar estrategias para hacer frente a estos riesgos y amenazas. En primer lugar, y en relación con el concepto de metaverso, es necesario establecer un espacio virtual seguro y estable para todos los usuarios. Los entornos virtuales, como el metaverso, están cada vez más interconectados con nuestra vida cotidiana, por lo que cualquier actividad perjudicial en dicho entorno repercutirá tanto en el usuario como en nuestro entorno real. Para ello, el papel de los desarrolladores y creadores es muy relevante, pudiendo establecer pautas comunitarias para evitar este tipo de situaciones a través de la monitorización constante del flujo de información, para eliminar y frenar el desarrollo de cualquier tipo de actividad que pueda dañar nuestra integridad y perturbar nuestra seguridad.

Además, y en relación con el desarrollo de actividades ilegítimas o la creación de comunidades y entornos para captar usuarios, se debe establecer una cooperación público-privada para vigilar y controlar los contenidos y la propaganda que se difunde *online*, limitándola o eliminándola si es posible. Al mismo tiempo, el desarrollo de campañas de sensibilización y la creación de manuales de buenas prácticas para los

usuarios permitiría a todos aquellos que deseen acceder al metaverso disponer de una base y unas normas de referencia que regulen inicialmente la actividad, actuando como un código de conducta. Del mismo modo, es importante la comunicación y denuncia de casos por parte de la comunidad, por lo que se deberían establecer canales de comunicación accesibles para evidenciar y hacerse eco de cualquier actividad que pueda ser considerada perjudicial.

Como vemos, la comunicación y el intercambio de información son necesarios para garantizar la seguridad tanto en entornos virtuales como reales. Al tratarse de un espacio nuevo, similar a nuestra vida cotidiana, los gobiernos y las organizaciones internacionales del ámbito de la seguridad y la defensa deben plantearse la aplicación y el desarrollo de estrategias y narrativas para contrarrestar la desinformación. Estas estrategias, que ayudarían a combatir la difusión de contenidos nocivos en el entorno virtual, ya han sido aplicadas anteriormente por organizaciones como la OTAN, ayudando a través de ellas a frenar la proliferación de la desinformación[6]. Estos trabajos, realizados en colaboración con otros miembros de la sociedad civil y organizaciones como el G7, Naciones Unidas o la Unión Europea, han sido valorados como esenciales para defender y mantener la seguridad pública[7], por lo que su aplicación en el metaverso puede ayudar a mantener el orden de la misma forma que en el entorno real, evitando cualquier posibilidad de contagio.

Por último, y a un nivel técnico que posteriormente puede dar lugar a una gran variedad de estrategias, se debe considerar la implementación de encriptación y otras herramientas técnicas que protejan a los usuarios tanto de la ciberdelincuencia como de las situaciones de peligro que puedan encontrar en el metaverso. El establecimiento de un marco de seguridad vigilado evitará que grupos extremistas, terroristas o cualquier usuario cuya voluntad no sea buena puedan atacar el entorno virtual, perturbando la paz y la seguridad del metaverso. En este sentido, considero relevante hacer uso de las guías y hojas de ruta existentes, ya sean propuestas por el sector público o privado, para mantener protegido el entorno virtual. Algunos ejemplos de textos que se pueden ampliar o utilizar como referencia para aplicar en el metaverso son *Countering Online*

[6] NATO. «NATO's approach to countering disinformation», *NATO* [en línea]. 2020. Disponible en: https://www.nato.int/cps/en/natohq/177273.htm [consulta: 22/2/2023].
[7] NATO. «NATO's approach to countering disinformation», *NATO* [en línea]. 2020. Disponible en: https://www.nato.int/cps/en/natohq/177273.htm [consulta: 22/2/2023].

Radicalisation del Centro Internacional para el Estudio de la Radicalización y la Violencia Política o *Metaverse; Implications for Security and Intelligence* de la NATO Foundation Defense College.

Repercusiones en el mundo real

Análisis del posible impacto de los riesgos y amenazas del metaverso en el mundo real

Tomando como referencia los ejemplos de amenazas y riesgos para la paz y la seguridad expuestos anteriormente, la exposición de un posible impacto de estos en el mundo real es más compleja de lo que parece.

Como consecuencia del rápido avance y constante cambio del metaverso, la ausencia de continuidad y largo recorrido es notable, especialmente con aquellos casos que pueden tomarse como referencia de tener impacto en nuestro mundo real.

Actualmente, hemos podido ser testigos de cómo conflictos que han tenido lugar en el entorno real, como es el caso del conflicto entre Rusia y Ucrania, han repercutido en el entorno virtual, afectando a las inversiones y mercados financieros de tókenes del metaverso o criptodivisas.

Estos casos ponen de manifiesto la posibilidad de reciprocidad de los conflictos entre ambos entornos, abriendo un abanico de posibilidades, especialmente para aquellos que ya tienen presencia en el ciberespacio. A continuación, se expondrán dos ejemplos en los que se aprecia claramente cómo las actividades que se desarrollan en el ciberespacio o en el metaverso tienen una alta capacidad de contagio en el mundo real.

En 2010, un grupo de investigadores alemanes descubrió cómo un gusano informático, un tipo de programa malicioso capaz de autorreplicarse y reubicarse en el entorno virtual, estaba asociado a los ataques perpetrados contra el programa y las instalaciones nucleares de Irán. El programa malicioso, denominado Stuxnet, abrió un nuevo capítulo de conflictos híbridos en los que los actos virtuales repercuten en el mundo real. Mediante la suplantación de identidad de dos empresas taiwanesas, los atacantes pudieron acceder tanto a infraestructuras iraníes, que eran el objetivo principal, como a infraestructuras estadounidenses o hindúes, de las que se informó de un impacto menor. Posteriormente se hizo público el objetivo de la operación, que trataba de obtener

información de parte de las instalaciones nucleares iraníes, concretamente las relacionadas con el programa ilícito de armas nucleares iraní. La clave de este ataque reside en la capacidad del atacante y del usuario virtual para matizar y ocultar esas características al ojo humano, es decir, en ningún momento este programa malicioso levantó sospechas en el entorno real, haciendo que el impacto fuera mucho mayor del deseado y cumpliendo su objetivo: tener la capacidad de afectar a infraestructuras críticas en el mundo real sin necesidad de realizar el ataque en persona, sino por medios virtuales.

Cabe señalar que el programa iraní ya había sido objeto de sanciones económicas y medidas diplomáticas. La falta de eficacia de estas motivó al usuario virtual, posiblemente relacionado con un entorno político (se llegó a considerar una operación conjunta entre Israel y Estados Unidos) a «tomar cartas en el asunto», implicando así al ámbito de las relaciones internacionales y los asuntos exteriores y poniendo en riesgo la paz y la seguridad internacionales.

En 2014, fue atacado el sistema de almacenamiento de información de la empresa de entretenimiento Sony. Este ataque, llevado a cabo por un grupo denominado «Guardianes de la Paz» robó información almacenada en la red de la compañía Sony a periodistas y medios de comunicación del entorno real, además de amenazar con medidas adicionales si la empresa de entretenimiento hacía pública la película *The Interview*, una comedia que ridiculizaba al régimen norcoreano. Teniendo en cuenta este contexto, podemos destacar cómo el grupo implicado fue identificado por el FBI como un grupo de *hackers* norcoreanos, que en todo momento actuaron en el entorno virtual, pero cuyas acciones tuvieron repercusión e impacto en el mundo real. Además de la denuncia pública y de la filtración de información de carácter privado, el gobierno estadounidense anunció la posibilidad de tomar medidas adicionales contra el país en caso de que los ataques persistieran, anunciando también sanciones contra Corea del Norte, en enero de 2015, como consecuencia del ataque contra Sony. Como vemos, a pesar de tratarse de un ataque *online*, la posibilidad de contagio y repercusión en el mundo real, y especialmente en materia de paz y seguridad, es muy alta.

Tanto el ataque a la infraestructura nuclear iraní como el ataque a Sony nos muestran dos escenarios y una nueva ventana de posibilidades de ataques en el entorno real

desde el mundo virtual. Aunque todavía es pronto para determinar el grado de contagio que se puede observar de las actividades del metaverso, en particular de los riesgos y amenazas, en el mundo real, estos ejemplos que han tenido un impacto considerable en el ciberespacio nos muestran que la posibilidad no es inexistente ni mínima, y que la ausencia de regulación y control sobre las actividades en este entorno, así como su diferenciación de las del mundo real, pueden poner en peligro nuestra paz y seguridad.

Conclusiones

El metaverso se está convirtiendo hoy en una realidad, pasando a formar parte integrante de nuestra vida cotidiana. Ante este nuevo escenario desconocido, nos enfrentamos a la posibilidad de nuevas amenazas que pongan en peligro nuestra paz y seguridad tal y como las conocemos.

Para hacer frente a estas situaciones, como se ha observado en este trabajo, es necesario desarrollar estrategias que hagan frente a estos riesgos y amenazas, garantizando la paz y la seguridad, estableciendo un entorno seguro y estable para todos los usuarios de este entorno virtual.

Mediante la aplicación de medidas de vigilancia, intercambio de información e inteligencia, cooperación y el establecimiento de un marco regulatorio en el entorno virtual, no solo podremos frenar y limitar el impacto de estas amenazas en el metaverso, sino que también podremos establecer un control sobre las mismas para evitar posibles contagios en la vida real.

No podemos negar que los gobiernos y las organizaciones internacionales se enfrentan a un nuevo paradigma que avanza más rápido de lo esperado, por lo que deben adaptarse a los retos que puedan surgir. En este aspecto, la innovación juega un papel muy importante, siendo más necesaria que nunca la cooperación público-privada y la creación de un espacio de diálogo que permita la elaboración de alternativas regulatorias, así como un metaverso descentralizado donde el poder y el control no se limiten a un único usuario o grupo. Asimismo, organizaciones como la Unión Europea, pueden jugar un papel muy relevante en el proceso de elaboración y creación de un marco regulatorio de las actividades en el metaverso, pudiendo así limitar el impacto de cualquier amenaza que se pueda contagiar al mundo real.

Ana María Martín Elvira
Consultora de Asuntos Públicos en ATERVIA
Estudiante del Máster de Geopolítica y Estudios Estratégicos, UC3M
@anamartinelv