BARATARIA
Revista Castellano-Manchega de Ciencias Sociales
Nº 35, pp. 28-38, 2024, ISSN: 1575-0825, e-ISSN: 2172-3184
DOI: https://doi.org/10.20932/barataria.v0i35.684

METAVERSO, CIBERESPACIO Y SEGURIDAD: LOS PROYECTOS DE CHINA Y JAPÓN

METAVERSE, CYBERSPACE AND SECURITY: CHINA AND JAPAN'S PROJECTS

Antonio César Moreno Cantano
Universidad Complutense de Madrid / España
antmor03@ucm.es
https://orcid.org/0000-0003-1008-2831

Recibido/Received: 26/11/2023
Modificado/Modified: 03/04/2024
Aceptado/Accepted: 15/04/2024

RESUMEN
Este artículo analiza cómo el poder militar de diferentes actores internacionales proyecta sus operaciones y capacidades operativas futuras a través del metaverso. Analizaremos la importancia de este elemento dentro del ciberespacio a partir de la teoría de la presión lateral. Para ello, nuestro marco metodológico se centrará en el estudio descriptivo y contextual de los principales planes de defensa de signo tecnológico de países como China y Japón. Como conclusiones, se puede resaltar la creciente preocupación internacional por el control del universo virtual por sus enormes potencialidades militares.

PALABRAS CLAVE
Metaverso; ejército; ciberespacio; Teoría de la Presión Lateral; tecnología.

SUMARIO
1. Introducción. 2. Marco teórico, estado de la cuestión y metodología. 3. Metaverso: implicaciones en defensa y seguridad. 4. Estudio de casos: China y Japón. 5. Conclusiones. Bibliografía.

ABSTRACT
This article analyzes how the military power, of different international actors, projects their future operations and operational capabilities through the metaverse. We will analyze the importance of this element within cyberspace based on the theory of lateral pressure. For this purpose, our methodological framework will focus on the descriptive and contextual study of the main technological defense plans of countries such as China and Japan. As conclusions, we can highlight the growing international concern for the control of the virtual universe due to its enormous military potentialities.

KEYWORDS
Metaverse; Military; Cyberspace; Lateral Pressure Theory; Technology.

CONTENTS
1. Introduction. 2. Theoretical framework, state of the art and methodology. 3. Metaverse: implications in defense and security. 4. Case studies: China and Japan. 5. Conclusions. References.

1. INTRODUCCIÓN

Años antes del desarrollo del metaverso, la comunidad virtual *Second Life* (Linden Lab, 2003) permitió a usuarios de todo el mundo interactuar expandiendo sus relaciones sociales. Diferentes marcas y compañías utilizaron este entorno para promocionar sus productos y alcanzar a mayor número de consumidores. Dentro de esta dinámica alcanzó un enorme éxito la isla creada por la *Australian Broadcasting Corporation*, la emisora nacional de Australia, financiada directamente por el gobierno del país. Sin embargo, en 2007 sufrió un ataque por parte de tres usuarios – catalogados en un primer momento como terroristas – y quedó completamente devastada. Posteriormente, los propios responsables de este espacio aclararon que la destrucción fue debida a un simple error informático y no a la acción humana (Stevens, 2015: 233). No sorprende que la primera reacción a esta acción fuera calificarla de atentado terrorista, pues existían precedentes de cómo diversos grupos extremistas se servían del medio cibernético para objetivos de adoctrinamiento, reclutamiento, comunicación y ensayo de ataques (Mandal & Lim, 2008). Con el objetivo de impedir este género de acciones, en EE.UU., bajo la dirección de la *Office of the Director of National Intelligence* (ODNI), se impulsó el *Reynard Project* (2008), primer caso en el que una agencia de inteligencia establecía una correlación entre avatares virtuales y su comportamiento en el mundo real (Vanorio, 2021). De esta manera, tanto la *CIA* como la *National Security Agency* abogaron desde 2008 por infiltrarse en los juegos en línea, como el famoso *World of Warcraft* o el referido *Second Life*, para controlar / denunciar las comunicaciones que diferentes grupos terroristas mantenían en estos espacios virtuales (Elliot, 2013). Años después, y gracias al avance tecnológico, el ciberespacio ha evolucionado hacia el concepto de metaverso, fortaleciendo – aún más- el interés de los agentes internacionales y el poder militar por controlar la seguridad en la red cibernética, más allá de temas vinculados únicamente al terrorismo, donde el énfasis se pone también en potenciar y mejorar futuras operaciones bélicas a través de la simulación y la gamificación (Der Derian, 2009).

La investigación, que centra este artículo, analiza y describe el creciente papel del metaverso como espacio virtual de desarrollo para los dilemas de seguridad y defensa de las Fuerzas Armadas de los principales agentes internacionales, con especial atención a China y Japón. Las preguntas que se formulan son:

- PI_1: ¿Cómo participa el metaverso dentro de la ciberpolítica? ¿Contribuye al dominio global de la interacción humana? Para responder a esta pregunta nos apoyaremos en interpretaciones y trabajos previos de Nazli Choucri (1989 y 2012), en especial en la *lógica de la presión lateral* y sus vínculos con el concepto de ciberespacio.
- PI_2: ¿Cuáles son los principales proyectos vinculados al metaverso por parte de las Fuerzas Armadas de las grandes potencias internacionales? Esta cuestión se enfoca al estudio descriptivo y al análisis contextual de las guías estratégicas en materias de Defensa y Tecnología de países como China y Japón. A partir de los modelos de Choucri (2012) sobre los dilemas que presenta el ciberespacio, se estudiará si estas iniciativas pueden dar respuesta y contribuir a reforzar todo el complejo de seguridad que implica el universo online, ahondando en sus potencialidades y limitaciones.

2. MARCO TEÓRICO, ESTADO DE LA CUESTIÓN Y METODOLOGÍA

El aumento del protagonismo de la tecnología en las últimas décadas ha provocado profundos

cambios en las estrategias de seguridad y de defensa de los diferentes agentes estatales en la sociedad internacional. Esto ha llevado, incluso, en algunos casos a hablar de "guerra tecnológica", como ejemplifica la creciente rivalidad entre EE. UU. y China en esta materia (Nung, 2022). En la presentación del número 208 de la revista *Política Exterior*, se resaltaba que "la tecnología es el factor definitorio de la actual reordenación del mundo", ya que entra de lleno "en la seguridad, los servicios públicos, la información o los medios de comunicación" (Moltó, 2022).

Dentro de la nueva configuración del orden internacional a través de la tecnología tenemos que destacar el ciberespacio. Su concepción, sus implicaciones en materia de seguridad y defensa y sus límites en el ámbito del Derecho Internacional llevan tiempo ocupando un lugar preponderante dentro de los debates teóricos de las Relaciones Internacionales (Patiño, 2019). Adelantándose a uno de los grandes retos con los que se vincula el metaverso en la actualidad, McEvoy (2010, p. 382) se interrogaba si el ciberpoder debe ser compartido por los Estados o cada uno de ello debe poseer el suyo propio. Para ello comparaba la interpretación del ciberespacio desde diferentes paradigmas, desde las narrativas liberales a las realistas. A través de categorías como territorio, poder e identidad, desgranaba las potencialidades y debilidades según cada uno de estos enfoques. Desde el realismo se destacaban algunos caracteres, y que serán de ayuda en nuestro propio análisis, como la identificación del ciberespacio como un reflejo de los poderes del mundo real; la presencia de peligrosos enemigos fronterizos virtuales; la necesidad de defensa de los ciudadanos por parte de los militares o las amenazas que existen protagonizadas por "comunidades virtuales imaginadas" (Yihadismo, por ejemplo) (McEvoy, 2010, p. 387). Hoy en día se aprecia que las cualidades del ciberespacio son tanto una fuente de desarrollo y progreso como de vulnerabilidad, así como una herramienta de control y de ataque, que representan una amenaza potencial para la seguridad y una perturbación del orden internacional conocido (Choucri, 2012, p. 3). Desde ese punto de vista, el ciberespacio es una de las principales zonas de disputa en política internacional. Para Joseph Nye, el ciberespacio incluye "la red de computadoras conectadas a internet, pero también incluye las redes internas (intranet), las tecnologías de telefonía móvil, cables de fibra óptica, comunicación satelital-espacial. Asimismo, el ciberespacio tiene una capa de infraestructura física que está sujeta a leyes económicas, leyes políticas de soberanía, competencia por recursos y por justificar su control y regulación" (2011, p. 19). La politóloga Nazli Choucri sintetizaba todos caracteres del ciberespacio en los siguientes ítems: *temporalidad* (instantáneo o casi instantáneo), *espacialidad* (trasciende límites geográficos), *extensión* (movilidad entre jurisdicciones), *participación* (menores barreras para el activismo y la participación política), *atribución* (se busca mantener oculta la identidad de las acciones) y *rendición de cuentas* (elude mecanismos de responsabilidad tradicional) (2012, p. 4). Como aporta Patiño (2019, p. 177), el sistema internacional cibernético presenta cuatro niveles de participación (individuales, grupales, estatales y sistémicos / globales) y cuatro dimensiones (jurídicas, económicas, políticas y seguridad). Uno de nuestros objetivos de investigación es analizar cómo el metaverso, como evolución presente de este sistema, permite a las Fuerzas Armadas adaptarse a los nuevos retos de seguridad. Siguiendo con las tesis de Choucri, este estudio recurrirá al concepto de la *presión lateral* (1989) aplicada al ciberespacio. La teoría de la presión lateral busca explicar las relaciones entre las características del estado y los patrones de comportamiento internacional. La teoría aborda las fuentes y consecuencias de la transformación y el cambio en las relaciones internacionales y proporciona una base para analizar posibles dinámicas de retroalimentación. La lógica de esta presión va desde los impulsores internos, las variables maestras que dan forma a los perfiles de los Estados a través de los efectos intermedios de demandas y capacidades institucionales socialmente agregadas y articuladas, hacia modos de

comportamiento externo diseñados para satisfacer las demandas dadas las capacidades disponibles. Dentro de estas demandas han ganado fuerza en los últimos años el control del ciberespacio, concebido como un dominio global de la interacción humana. Como apunta Choucri (2012), este nuevo ámbito de interacción es una fuente de vulnerabilidad, una amenaza potencial a la seguridad nacional y una perturbación del orden internacional familiar. Se generan, consecuentemente, tres imperativos principales sobre el ciberespacio: 1) *Desafíos al sistema estatal*; 2) *Dilemas de seguridad emergentes*; 3) *Perfiles estatales: "reales" y cibernéticos*. La nueva normalidad en la política mundial trasciende las agencias estatales e incluye una amplia gama de actores no estatales, conocidos o no, que operan en un contexto internacional altamente dinámico y volátil. En segundo lugar, este limita la eficacia de las nociones tradicionales de disuasión: el concepto y la práctica. La tradición supone el conocimiento de la identidad del adversario, condición que muchas veces no se cumplen en el presente. Todo esto crea un desafío general e ineludible para el Estado, el sistema estatal y las relaciones internacionales. El desafío es cómo gestionar todo el complejo de seguridad, dada la aparición de formas sin precedentes de amenazas a la seguridad (ciberamenazas) que señalan nuevas vulnerabilidades (que socavan la ciberseguridad) y –lo más desconcertante de todo– que emanan de fuentes desconocidas (una característica a la que nos referimos como el problema de la atribución). Todo esto refuerza inevitablemente la politización del ciberespacio y su prominencia en los discursos políticos emergentes. Finalmente, Choucri (2012) nos plantea dos cuestiones fundamentales: ¿los perfiles estatales en el ámbito cibernético reflejan los del mundo tradicional o "real"? y ¿los patrones de cambio observados en la ubicación de un Estado en el "espacio" de perfil "real" son similares a los del dominio cibernético? Son desafíos a los que se enfrentan las políticas militares de las grandes potencias internacionales en el metaverso. Para intentar dar respuesta, analizaremos si las guías estratégicas en materia de tecnología y seguridad de diferentes agentes estatales destacados en el ámbito del ciberespacio, como China y Japón, tienen en cuenta todos estos factores e intentar explicar cómo se articulan sus acciones en el mundo virtual interconectado. Por razones de espacio será imposible abordar otros casos, si bien el lector podrá encontrar referencias interesantes a diversos estudios geográficos en las investigaciones de Gruszczack y Kaempf (2023).

3. METAVERSO: IMPLICACIONES EN DEFENSA Y SEGURIDAD

A lo largo de la historia, la guerra ha estado determinada por factores geopolíticos, sociales, económicos, militares y tecnológicos. Estos elementos también aparecen en el debate actual sobre el futuro de la guerra, un debate desencadenado por los acontecimientos relacionados con la Cuarta Revolución Industrial. Esta revolución se apoya fundamentalmente en lo digital, pero no es simplemente una expansión de ella. La Cuarta Revolución Industrial difumina la distinción entre los ámbitos físico, digital y biológico. Los avances tecnológicos emergentes en áreas tan diversas como la inteligencia artificial, la robótica, el Internet de las Cosas (IoT, en sus siglas inglesas), la impresión tridimensional, la nanotecnología y la informática cuántica, afectan profundamente a todos los aspectos de nuestra sociedad (Schwab, 2016). Al igual que las revoluciones anteriores que remodelaron la sociedad y transformaron el carácter de la guerra, la actual también está trayendo cambios significativos en la forma en que los ejércitos modernos se entrenan, organizan y llevan a cabo las operaciones (Raska et. al., 2022).

El metaverso es una forma de realidad que combina aspectos de las redes sociales, el IoT, la Realidad Aumentada (RA) y la Realidad Virtual (RV) para permitir a sus usuarios interactuar virtualmente. Es un concepto de universo tridimensional persistente que combina

espacios virtuales en los que los usuarios pueden reunirse, trabajar y socializar. Es importante señalar que el término no se refiere a un tipo específico de tecnología, sino más bien a una nueva forma de interactuar con las tecnologías digitales existentes. La evolución del metaverso implica tres fases: los "gemelos digitales", los "residentes digitales" y, por último, la "surrealidad". El metaverso es un espejo digital del mundo físico y los gemelos digitales son los pilares de esta nueva realidad. Los gemelos digitales son réplicas digitales de físicas, productos, procesos y sistemas. Proporcionan una conexión entre una entidad física y su homólogo virtual. La conexión se establece mediante sensores que intercambian datos en tiempo real. Los gemelos digitales reflejan una reproducción digital realista del mundo tangible. El gemelo digital de un objeto nos permite recrearlo completamente con datos en directo, pero también evaluarlo y reinsertarlo en el sistema. La realidad y la virtualidad coexisten como dos espacios paralelos. En la segunda fase participan los residentes digitales, los representantes digitales en el mundo virtual, que desarrollan contenidos. Prácticamente son los avatares digitales que producen percepciones en los espacios virtuales. La última fase es la de la surrealidad, en la que una versión madura del metaverso absorberá gradualmente la realidad. Los usuarios vivirán e interactuarán con los objetos virtuales integrados en el metaverso. Tecnología holográfica avanzada y los monitores de alta calidad difuminarán la diferencia entre lo real y lo virtual, materializando así un estado de surrealidad. Del mismo modo que Internet sirvió de columna vertebral del ciberespacio, el metaverso podría funcionar como el medio que nos permitirá experimentar un nuevo dominio y una nueva realidad, creados por mundos virtuales interconectados. Esta evolución afectará profundamente al funcionamiento de las sociedades, las economías y los gobiernos, así como al entrenamiento y la lucha de los ejércitos (Liaropoulos, 2023, pp. 310-311). Organismos como la OTAN, recurriendo incluso a la ciencia ficción, ha intentado imaginar cómo se desarrollarían las guerras futuras, qué elementos tecnológicos estarían presentes. En ese sentido, y a través de la *Allied Command Transformation*, publicó en 2016 la novedosa obra *Visions of Warfare 2036*, donde jugaba con la distopía como escenario de simulaciones, donde el componente virtual tendría un lugar muy relevante (Mirrlees, 2023, p. 76).

Sin embargo, el camino hasta llegar a este punto ha sido largo e intenso. Hace más de 40 años, en 1978, el capitán de la USAF, Jack Thorpe, imaginó redes de simuladores que se utilizarían para la planificación, ensayo y ejecución del combate. En su artículo: Visiones futuras: entrenamiento de tripulaciones aéreas 1980-2000, previó que los sistemas de simulación y misión se unirían y "alinearían estrechamente los sistemas de entrenamiento con la preparación real para el combate y los harían indistinguibles". Thorpe pasó a liderar el programa SIMNET (Simuladores en Red) de DARPA (Agencia de Proyectos de Investigación Avanzada de Defensa de EE.UU.), que a finales de la década de 1980 culminó en más de 200 simuladores de tanques y aviones en red local y de área amplia conectados dentro de los EE.UU. y Europa. Para reducir el tráfico de la red, se compartió un único "modelo mundial" básico unificado entre todos los simuladores, cada uno de los cuales calcularía su propio estado y transmitiría las correcciones al modelo mundial según fuera necesario. Los enfoques desarrollados en ese momento llevaron al protocolo de Simulación Interactiva Distribuida (DIS), todavía en uso hoy en día. No se trataba sólo de la interconexión de mundos virtuales. A principios de la década de 1990, junto con la Marina de los EE. UU., DARPA conectó en red el *USS Wasp*, en el puerto de Norfolk (Virginia), con helicópteros simulados SIMNET del Cuerpo de Marines en Fort Rucker (Alabama), tanques del Ejército simulados, centros de mando del personal de la Marina y un nodo de observación en el Instituto de Análisis de la Defensa. La tripulación del Wasp pudo "detectar" los helicópteros simulados y los pilotos pudieron ver el barco simulado. Después de SIMNET, los militares continuaron adoptando la

idea de unir los mundos real y virtual. En 1999, el Ministerio de Defensa del Reino Unido definió los entornos sintéticos como la vinculación de "una combinación de modelos, simulaciones, personas y equipos reales en una representación común del mundo que proporciona coherencia y concurrencia a través de actividades previamente discretas". En 2007, el entonces Jefe del Estado Mayor de Defensa del Reino Unido, Sir Jock Stirrup, expresó que "la tripulación de un submarino cuando está sumergido ya está operando en muchos sentidos en un entorno virtual... y podemos ver cómo emerge la fusión del mundo sintético y el real en entornos tales que haría cada vez más difícil distinguir entre el entrenamiento realizado en simulación y el real". En julio de 2020, la líder del Equipo Transfuncional de Entorno de Entrenamiento Sintético del Ejército de EE. UU., Mayor General María Gervais, dijo que el objetivo de su equipo era establecer un entorno sintético común, donde se pueda realizar entrenamiento en vivo, virtual y constructivo a través de "estándares comunes, datos comunes, terreno común y una arquitectura abierta" (Fawkes, 2020).

El ejército británico también ha estado investigando el uso de la tecnología XR (Realidad extendida o tecnologías inmersivas, que incluye realidad virtual, realidad aumentada y realidad mixta) a escala, con más de 30 soldados en el mismo escenario de entrenamiento virtual. Quizás el proyecto más ambicioso para simular todo el espacio de batalla es el Entorno Sintético Único (SSE) del Ministerio de Defensa del Reino Unido que, inspirado en la tecnología SpatialOS de Improbable (que permite simulaciones a gran escala), tiene como objetivo aprovechar los avances tecnológicos en los videojuegos e Internet. Reconoce que el mundo se ha vuelto cada vez más interconectado y está impulsado por datos y, por lo tanto, es más difícil para los tomadores de decisiones comprender, visualizar y responder rápidamente. Según el documento "Detalle de oportunidad" del Ministerio de Defensa SSE, se construirá un "gemelo digital" del mundo real con igual complejidad "como medio para aprovechar el desafío, visualizar lo oculto y transformar el apoyo a la toma de decisiones" (Fawkes, 2020).

Las potencialidades del metaverso, en campos como la Educación (Sánchez-López et. al., 2022) o el ámbito empresarial (Periyasamy & Periyasamy, 2023), son numerosas. Con respecto al ámbito militar, organismos como la OTAN han publicado en fecha reciente destacados estudios donde han sido analizadas detalladamente. Por supuesto, se esbozan muchos proyectos futuros que deben ser ideados e implementados aún, pero nos sirven para tener un conocimiento más amplio de este tema. Siguiendo la investigación de Solly y McArdle (2022), encontramos cinco grandes atribuciones: 1) Desarrollo de capacidades; 2) Adquisiciones; 3) Formación y educación; 4) Apoyo a las operaciones militares, y 5) Ensayo de misiones. De manera específica se distribuirían en las siguientes actividades:

a. Simulaciones de entrenamientos virtuales mediante la combinación de RV, RA e Inteligencia Artificial,
b. Control remoto de sistemas de armas y visualización de datos del campo de batalla en tiempo real,
c. Formación médica mejorada con realidad virtual,
d. Capacitación en mantenimiento de equipos virtuales,
e. Ejercicios de guerra cibernética y entrenamiento de operaciones militares conjuntas,
f. Escenarios de respuesta a desastres y simulaciones de juegos de guerra,
g. Entrenamiento de resiliencia psicológica y reconocimiento y Vigilancia,
h. Reclutamiento e Incorporación y colaboración y planificación remotas,
i. Formación Lingüística y Cultural y relaciones Públicas y divulgación.

Elementos todos ellos que darán al poseedor y controlador del metaverso una ventaja de primera magnitud en las confrontaciones de las próximas décadas. Eso explica el interés

creciente de diferentes países por invertir y desarrollar en esta tecnología virtual.

4. ESTUDIO DE CASOS: CHINA Y JAPÓN

4.1. China

El desarrollo tecnológico es uno de los principales pilares del plan estratégico *Made in China 2025* impulsado por el presidente Xi Jinping. Este ambicioso proyecto, categorizado dentro de una estrategia global de "tecnosocialismo y capitalismo de Estado" (González, 2021, p. 21), pretende convertir al país en dicha fecha en líder de industrias como la robótica o la inteligencia artificial, entre otras muchas. Recientemente, el Partido Comunista Chino fue más lejos y señaló el año 2035 como momento clave en el que China se haya convertido "en una gran nación socialista, moderna, próspera y poderosa, autosuficiente tecnológicamente y capaz de liderar al mundo" (Ambrós, 2020). El interés por la tecnología del actual mandatario chino se puede remontar al año 2000, cuando siendo secretario del comité del Partido de Zhengding (en Hebei) expresó que "la tecnología es la clave y la información es el alma" de la nación. Años después, y ya como líder, profundizó en esta idea con las siguientes palabras:

> "Para que China crezca fuerte, próspera y rejuvenecida, sin duda necesitamos desarrollar la ciencia y la tecnología a lo grande. Debemos esforzarnos por convertirnos en el principal centro mundial de la ciencia y la innovación. Estamos más cerca que nunca en la historia del objetivo del gran rejuvenecimiento de la nación china, y necesitamos más que nunca convertir a China en una superpotencia mundial de ciencia y tecnología" (Baughman, 2022a, p. 3).

Estos planes de desarrollo tecnológico se insertan en un plan global de Defensa conocido como la *Estrategia de las Tres Guerras*, que busca un marco general favorable a la República Popular China en el ámbito psicológico (*psychological milieu*) que influirá decisivamente en cómo operan los actores internacionales en el ámbito del mundo real (*operational milieu*). Las Tres Guerras es un enfoque estratégico dinámico y matizado para influir en las operaciones que consta de tres elementos interrelacionados: guerra psicológica, guerra de opinión pública y guerra legal. El propósito de las Tres Guerras es establecer un "poder discursivo" sobre un adversario: el poder de controlar las percepciones y dar forma a las narrativas que sirven a los intereses chinos, al tiempo que socavan los de un oponente (García Cantalapiedra, 2022, p. 11). Este tipo de maniobras se extienden, por supuesto, a Internet y a los nodos virtuales. En este sentido, y previo paso al desarrollo de los primeros proyectos sobre el metaverso militar, en 2016 se implementó una ambiciosa estrategia de Seguridad Nacional sobre el Ciberespacio:

> "Salvaguardar la ciberseguridad de nuestro país es una medida importante para avanzar en el acuerdo estratégico de construir integralmente una sociedad modestamente acomodada, profundizar integralmente la reforma, gobernar integralmente el país de acuerdo con la ley y gobernar integral y estrictamente al Partido de manera coordinada, y es una garantía importante para realizar el objetivo de la lucha de los 'Dos Centenarios' y hacer realidad el sueño chino del gran rejuvenecimiento de la nación china" (Creemers, 2016).

Este plan, y siguiendo los planteamientos de Choucri, pretendía hacer frente a los principales retos del ciberespacio: desafíos al sistema estatal; dilemas de seguridad emergentes; y perfiles estatales: "reales" y cibernéticos. Para ello proponía tres tareas estratégicas: 1) Defender decididamente la soberanía en el ciberespacio; 2) Salvaguardar resueltamente la

seguridad nacional; y 3) Proteger la infraestructura de información crítica (Creemers, 2016). Los puntos uno y dos implican la participación del Ejército Popular de Liberación chino en el mundo virtual, el metaverso. Para impulsar la innovación del estamento militar, Xi Jinping firmó la orden de movilización de entrenamiento de 2021 de la Comisión Militar Central para «fortalecer la construcción de medios de simulación, redes y confrontación online». Este metaverso militar, llamado *Battleverse*, se edificará sobre un ejército virtual, el "Ejército azul", que simule todos los aspectos de un conflicto potencial, imitando perfectamente el comportamiento de toma de decisiones del comando del enemigo (Baughman, 2022b). Desde los medios escritos oficiales militares chinos, se destacó el potencial del metaverso para una futura guerra cognitiva, que enlaza con la idea de la importancia de las narrativas estratégicas y el poder discursivo en materia de geopolítica y seguridad. A diferencia del efecto unidireccional de tecnologías individuales como la inteligencia artificial y las redes de información sobre el pensamiento y la cognición, el metaverso -según las autoridades chinas- proporciona un espacio mutuamente construido de interacción y contraefecto, influencia y contrainfluencia entre tecnología y cognición. El metaverso proporciona un espacio cognitivo paralelo que es un gemelo digital de escenarios de combate reales, donde la guerra cognitiva puede promoverse de manera eficiente, mejorarse a un ritmo rápido y presentarse de manera panorámica (Dongheng et. al. 2022). Los beneficios del *Battleverse*, tal y como apuntamos de manera genérica en el punto tres al referirnos a las potencialidades militares del metaverso, oscilan entorno a cinco campos. El primero es la educación. El *battleverse* desempeñará un papel importante en la educación centralizada, permitiendo la libre comunicación con profesores y alumnos con independencia de su ubicación. Las herramientas de enseñanza virtual también mejorarán la capacidad del profesor para explicar nuevos conceptos. Segundo, formación. Capacidad para satisfacer plenamente los requisitos reales de combate en el contexto de una operación a gran escala.

El entrenamiento y las evaluaciones repetidas ayudarán a perfeccionar la cooperación táctica y la voluntad de lucha de los soldados. La evaluación será más cuantitativa y ayudará a discernir rápidamente a los soldados con más talento. Tercero, pruebas. Las nuevas armas pueden probarse en simulaciones para evaluar su rendimiento, compatibilidad y eficacia general en combate. Cuarto, investigación. Coordina los recursos de expertos sin importar su ubicación física. Es una plataforma de deducción y verificación a distancia de nuevos equipos e innovación de tácticas. Permite la realización de análisis continuos y obtención de conjuntos de datos masivos para analizar y cumplir los objetivos de investigación. Finalmente, comunicación de apoyo. Si los medios normales de comunicación del mando se destruyen en una batalla, el *battleverse* puede actuar como sistema de comunicación de reserva (Baughman, 20221, p. 8). Todo un elenco de posibilidades que pueden convertir al metaverso en un nuevo escenario de competencia global entre las grandes potencias.

4.2. Japón

A finales de 2022, el gobierno de Fumio Kishida hizo público tres documentos estratégicos para abordar los retos de seguridad en la región: la Estrategia de Seguridad Nacional (NSS), la Estrategia de Defensa Nacional y el Programa de Refuerzo de la Defensa. En todos estos planes se decidió revisar niveles relacionados con las capacidades de defensa, tecnológicas o cibernéticas. Aspectos que ya habían adquirido una relevancia de primera magnitud en el informe gubernamental de 2007 titulado *Innovation 25*. Ante el riesgo de quedar rezagada en la carrera tecnológica de las grandes potencias (en especial referencia a China y EE.UU., sin olvidar el papel de otros actores internacionales como Corea del Sur), se idearon toda una serie de medidas con las que mejorar el posicionamiento de Japón ante los nuevos retos futuros a

nivel global. En el epígrafe «Una sociedad abierta al mundo» indicaban la necesidad de desarrollar la tecnología virtual por sus múltiples potencialidades (Innovation 25). Esta preocupación aparecía también recogida en la referida *Estrategia de Defensa Nacional*. En el capítulo 7 señalaban la fuerte vinculación que se establecía entre tecnología y defensa para asegurar el porvenir de la nación y hacer frente a "nuevas formas de guerra". Para reforzar esta arquitectura de defensa era indispensable aumentar los fondos en I+D y hacer partícipe a la sociedad civil para la transferencia de conocimiento hacia el ámbito militar: desde grupos de investigación a universidades o mediante la colaboración de compañías privadas. Todos estos fines se regularían a partir del departamento ATLA (Acquisition, Technology and Logistics Agency), que en el futuro plantearía respuesta a los nuevos retos, entre otros, del ciberespacio y la ciberseguridad (Ministry of Defense, 2022: 33-34).

Estos aspectos han encontrado muy recientemente una mayor concreción en la *Guía de Defensa Tecnológica* (junio de 2023), enfatizando la necesidad de adaptarse a las tecnologías en evolución en la guerra moderna. Esta directiva identificó doce prioridades clave para alrededor de 200 empresas seleccionadas que participan en la iniciativa de tecnología de defensa del país. En particular, estas líneas de actuación primordiales abarcaban conceptos como "visualización de cosas invisibles" y "capacidades que convierten la información virtual/imaginaria en cosas reales", aspectos que se pueden vincular directamente con el metaverso militar. En el caso japonés, existen toda una gama de impulsores internos (desarrollo económico) y demandas externas (rivalidades por el control del ciberespacio y dilemas de ciberseguridad que de él se derivan) que han animados a los dirigentes del país a apostar por este nuevo campo de desarrollo tecnológico. Existe una "presión lateral", en materia de seguridad y defensa (principalmente), que determinan las actitudes del agente estatal. De esta manera, Japón necesita hacer frente a la competencia que la Fuerza de Apoyo Estratégico del Ejército Popular de Liberación de China está impulsando a nivel tecnológico y digital con el fin de asentar su territorialidad en el Mar de China Meridional.

5. CONCLUSIONES

El avance tecnológico de las últimas décadas ha propiciado el desarrollo del ciberespacio, que junto a enormes aspectos positivos (inmediatez, simulación, interactividad, control) también ha provocado múltiples dilemas de seguridad y defensa relacionados con el terrorismo, el robo de datos o ataques virtuales a sistemas informáticos prioritarios. Desde la perspectiva teórica del sistema internacional, su definición, características e interpretaciones, ha generado una enorme literatura y profundos debates según el paradigma interpretativo desde el que se plantee (desde el liberalismo al realismo). Una de las tesis más interesantes y que ha convertido al ciberespacio en el eje de la geopolítica internacional es la lógica de la presión lateral de la politóloga Nazli Choucri, que lo califica como un dominio global de la interacción humana. Debido a sus particularidades (*temporalidad, espacialidad, extensión, participación, atribución* y *rendición de cuentas*), el ciberespacio se encuentra sometido a toda serie de amenazas y retos que obligan a los agentes internacionales a actualizar sus medidas de ciberseguridad, dando un mayor protagonismo, en sus estrategias tecnológicas defensivas, al universo virtual. Desde finales de los años 90, en especial de EE.UU. y Reino Unido, a través de programas como SIMNET, el entorno virtual ha sido empleado de manera creciente por el estamento militar para llevar a cabo simulaciones de tácticas de guerra, con fines formativos o predecir comportamientos en escenarios bélicos. Aspectos todos ellos que en la actual revolución tecnológica han desembocado en el metaverso que, gracias a la combinación de la

RV, RA o el IoT, permiten ampliar todo ese campo de posibilidades.

El análisis del caso chino y japonés (líderes junto a EE.UU., en la industria digital a nivel global), a través de la aproximación de sus principales guías y estrategias de defensa y seguridad en materia tecnológica, indican la necesidad de dotar a las fuerzas armadas de nuevos mecanismos para desplegar todas sus facultades en el ciberespacio. China está impulsando un revolucionario proyecto virtual, a través del *Blue Army*, que le permitirá contar en un futuro cercano con un metaverso militar, el *Battleverse*, que jugará un papel decisivo en las próximas guerras cognitivas. Es ese especial escenario, el de la "visualización de cosas invisibles" y "capacidades que convierten la información virtual/imaginaria en cosas reales" -como recogen los planes oficiales tecnológicos nipones -, el que permitirá dotar de las habilidades necesarias a los ejércitos del siglo XXI. Simular la realidad para que lo virtual permita imponerse en los escenarios globales. Son proyectos aún en un estadio muy prematuro, pero a los que se destinan gran cantidad de medios, incluyendo la participación de compañías privadas que puedan aportar su experiencia tecnológica desde otros ámbitos. A los civiles nos queda observar -desde el plano físico o virtual- si los conflictos venideros se desarrollarán en formato digital o a través de realidades paralelas a la real.

BIBLIOGRAFÍA

Ambrós, I. (2020). 'La hoja de ruta china para liderar el mundo'. *Política Exterior*. https://www.politicaexterior.com/la-hoja-de-ruta-china-para-liderar-el-mundo/

Baughman, J. (2022a). Enter the Battleverse: China´s Metaverse War. *Military Cyber Affairs* 5(1): 1-15. https://digitalcommons.usf.edu/mca/vol5/iss1/2

Baughman, J. (2022b). China is Building a Blue Army in the Metaverse. *MCPA*. https://public.milcyber.org/activities/magazine/articles/2022/baughman-china-blue-army-metaverse

Creemers, R. (Ed.) (2016). National Cyberspace Security Strategy. *China Copyright and Media*. https://chinacopyrightandmedia.wordpress.com/2016/12/27/national-cyberspace-security-strategy/

Choucri, N., & North, R. C. (1989). Lateral pressure in international relations: Concept and theory, en M. I. Midlarsky (Ed.), *Handbook of war studies* (pp, 289–327). University of Michigan Press.

Choucri, N. (2012). *Cyber Politics in International Relations*. MIT Press.

Der Derian, J. (2009). *Virtuous War: Mapping the Military-Industrial-Media-Entertainment Network.* Routledge.

Dongheng, C., Chan, D. & Yaru, F. (2022). *The Metaverse: The New Heights of Future Cognitive War* [元宇宙：未来认知战的新高地]. https://www.workercn.cn/c/2022-03-03/6765828.shtml

Elliot, J. (2013). World of Spycraft: NSA and CIA Spied in Online Games. *ProPublica*. https://bit.ly/3AoaSi7

Fawkes, A. (4 de noviembre, 2020). Has the Military Been Building the Metaverse? *Halldale Group*. https://www.halldale.com/articles/17827-has-the-military-been-building-the-metaverse

García Cantalapiedra, D. (2022). La Estrategia de las Tres Guerras: la Guerra Política con características chinas dentro de la Gran Estrategia de la República Popular de China. *Instituto de Estudios Estratégicos. Documento de opinión*. https://www.ieee.es/Galerias/fichero/docs_opinion/2022/DIEEEO29_2022_DAVGAR_China.pdf

González, C. (2021). *El gran sueño de China. Tecno-socialismo y capitalismo de Estado*. Tecnos.

Gruszczak, A. & Kaempf, S. (2023). *Routledge Handbook of the Future of Warfare*. Routledge.

Innovation 25 (2007). *Creating the Future, Challenging Unlimited Possibilities. Executive Summary*. Prime Minister of Japan and His Cabinett. https://japan.kantei.go.jp/innovation/interimbody_e.html

Liaropoulos, A. (2023). Digitizing the Battlefield. Augmented and Virtual Reality Applications in Warfare, en A. Gruszczak, A. & S. Kaempf, (2023). *Routledge Handbook of the Future of Warfare* (pp. 308-311). Routledge.

Mirrlees, T. (2023). Militainment for Future Warfare, en A. Gruszczak & S. Kaempf (2023). *Routledge Handbook of the Future of Warfare* (pp. 74-84). Routledge.

McEvoy, M. (2010). From Global Village to Virtual Battlespace: The Colonizing of the Internet and the Extension of Realpolitik. *International Studies Quarterly* 54: 381-401. https://doi.org/10.1111/j.1468-2478.2010.00592.x

Moltó, Á. (2022). 'El factor tecnológico. Carta a los lectores'. *Política Exterior*, 228 (julio-agosto). https://www.politicaexterior.com/articulo/el-factor-tecnologico/

Ministry of Defense (2022). *National Defense Strategy. Japan*. https://www.mod.go.jp/j/policy/agenda/guideline/strategy/pdf/strategy_en.pdf

Nung, P. (2022). *Techno-Geopolitics. US-China Tech War and the Practice of Digital Statecraft*. Routledge.

Nye, J. S. (2011). Nuclear lessons for cyber security? *Strategic Studies Quarterly*, 5(4): 18-38. https://www.jstor.org/stable/26270536

Patiño Orozco, G. A. (2019). El sistema internacional cibernético: elementos de análisis. *Oasis*, (30): 163–186. https://doi.org/10.18601/16577558.n30.10

Periyasamy, A. & Periyasamy, S. (2023). Rise of digital fashion and metaverse: influence on sustainability. *DESD* 1(16): 1-26. https://doi.org/10.1007/s44265-023-00016-z

Raska, M., Zysk, K. & Powers, I. (2022). *Defence Innovation and the 4th Industrial Revolution.* Routledge

Sánchez-López, I., Roig-Vila, R. & Pérez-Rodríguez, A. (2022). Metaverse and education: the pioneering case of Minecraft in immersive digital learning. *Profesional de la información*, 31 (6): 1-17. https://doi.org/10.3145/epi.2022.nov.10

Schwab, K. (2016). *The Fourth Industrial Revolution.* Penguin Random House.

Solly, R. y McArdle, J. (2022). Unlocking the Military Potential of the Metaverse. *NATO*. https://www.sto.nato.int/publications/STO%20Meeting%20Proceedings/STO-MP-MSG-197/MP-MSG-197-27P.pdf

Stevens, Tim (2015). Security and surveillance in virtual words: Who´s watching the warlocks and why? *International Political Sociology* 9(3): 230-247. https://doi.org/10.1111/ips.12094

Sujoyini M. & Lim, E. (2008). Second Life: Limits of Creativity or Cyber Threat? *IEEE Conference on Technologies for Homeland Security*, Waltham, MA, USA, 498-503. https://doi.org/10.1109/THS.2008.4534503

Vanorio, F. (2021). Metaverso e Sicurezza Nazionale. *Istituto Italiano Di Studi Strategici*. https://www.strategicstudies.it/wp-content/uploads/2021/12/Edizioni-Machiavelli-Metaverso-e-Sicurezza-Nazionale.pdf

Breve currículo:

Antonio César Moreno Cantano
Doctor en Historia Contemporánea. Profesor Asociado en el Departamento de Relaciones Internacionales e Historia Global de la Universidad Complutense de Madrid. Miembro del Grupo de investigación *Seguridad, Desarrollo y Comunicación en la Sociedad Internacional* de la UCM (UCM-971010-GR96/20). Acreditación ANECA a la figura de Profesor Titular (rama de Humanidades). Su principal línea de investigación es la geopolítica internacional y los *Digital Games*. Su última publicación es: International Geopolitics and Digital Games in the Nationalist Agenda of Great Powers, en C. Bjola & I. Manor (Eds.). (2023). *The Oxford Handbook of Digital Diplomacy*. Oxford University Press.