ESCUELA NAVAL DE CADETES
"ALMIRANTE PADILLA"
Honor y Tradición

REVISTA DERROTERO

Defensa y Seguridad

Juegos de Guerra como Apoyo a la Gestión Estratégica de la Ciberdefensa en Colombia: Revisión Sistemática de Literatura[1]

War Games as Support to the Strategic Management of Cyber Defense in Colombia: Systematic Review of Literature

Juan Carlos Camilo García Ruiz[2]
Diego Edison Cabuya Padilla[3]

Recibido: 07/03/2022
Aprobado: 08/05/2022

Correspondencia: diego.cabuya@armada.mil.co

Resumen

El presente artículo tiene como objetivo evidenciar la importancia de los juegos de guerra en la gestión de la ciberdefensa y la ciberseguridad, mediante el uso de herramientas didácticas (aprender jugando) y ambientes seguros que permitan realizar pruebas en todos los niveles de la gobernanza cibernética, generando insumos para la toma de decisiones y así tener un panorama más amplio del entorno en el ciberespacio. Para lo anterior se establecieron dos fases, la primera trató de una revisión sistemática de la literatura sobre los juegos de guerra en ciberseguridad y ciberdefensa, utilizando un análisis bibliométrico para determinar la producción científica y tendencias de la temática, dando como resultado que las investigaciones en temas de ciberdefensa y ciberseguridad vienen en aumento, principalmente en simulación y gamificación enfocada a la ciberdefensa. Sin embargo, la producción es baja y no es posible identificar una tendencia clara de metodologías. En la segunda fase se caracterizaron los principales juegos de guerra en ciberdefensa que son juegos de mesa y juegos de roles. Finalmente, se concluye que los juegos de guerra son parte clave en el análisis de escenarios operacionales de ciberdefensa, sin embargo, la producción científica es poca alrededor del tema, lo que genera mayores oportunidades de investigación en este tema.

1 El presente artículo de investigación es presentado como opción de grado para optar al título de Magíster en Ciberseguridad y Ciberdefensa de la Escuela Superior de Guerra, siendo producto del proyecto de investigación titulado "Juegos de Guerra como apoyo a la Gestión Estratégica de la Ciberdefensa en Colombia: Revisión Sistemática De Literatura.", vinculado al grupo de investigación Masa Crítica, categorizado en B COL0123247, inscrito en Minciencias.

2 Oficial Naval Armada de Colombia, de grado Capitán de Corbeta, Escuela Superior de Guerra "Brigadier General Rafael Reyes Prieto", Bogotá, Colombia. Ingeniero de Sistemas con énfasis en telecomunicaciones. Especiales en seguridad de la Información. Certificado Ethical Hacker v9.

3 Oficial Naval Armada de Colombia, de grado Capitán de Corbeta, Escuela Superior de Guerra "Brigadier General Rafael Reyes Prieto", Bogotá, Colombia. Ingeniero Electrónico, Máster en Gestión de la Información.

Palabras Claves: Bibliometría, juegos de guerra, gamificación, ciberdefensa, simulación.

Abstract

This article aims to highlight the importance of war games in the management of cyber defense and cyber security, this with the use of didactic tools "learn by playing", safe environments that allow testing at all levels of cyber governance , generating inputs for decision making and thus have a broader picture of the environment in cyberspace; The foregoing was carried out in the first phase in a systematic review of the literature on war games, using a bibliometric analysis to measure its quality, production and impact and to have a roadmap that allows us to characterize the different war games and their lines. of action. As a result of this process, it can be shown that even though research on cyber defense and cyber security is on the rise, issues related to war games, simulation and gamification focused on cyber defense are still incipient, and there are different lines of action in games. of war without having a defined standard and where kinetic models are taken and overlapped to the cybernetic field, which does not always turn out to be successful.

Key Words: bibliometrics, war games, gamification, cyber defense, simulation.

Introducción

La Cuarta Revolución Industrial ha profundizado la globalización, caracterizada por la aparición de nuevas tecnologías que están fusionando el mundo físico, digital y biológico (Schwab, 2016). La masificación de internet y el creciente acceso por parte de múltiples actores, al igual que la expansión de las relaciones humanas a entornos digitales no convencionales, ha derivado en la creación del ciberespacio (Singer & Friedman, 2013) que se aceleró de forma exponencial en el año 2020, en el marco de la pandemia COVID-19, cuando se redujo el contacto físico de las personas, pero se mantuvieron las actividades propias de la sociedad.

El creciente aumento de usuarios de internet y la elevada dependencia de la infraestructura crítica nacional hacia los medios electrónicos, han visibilizado un aumento en los incidentes y delitos contra la seguridad y defensa cibernética, evidenciando el elevado nivel de vulnerabilidad del país ante amenazas cibernéticas, tales como el uso de internet con fines terroristas, el sabotaje de servicios, espionaje y hurto por medios electrónicos, entre otros.

Los desafíos de la defensa contra las violaciones de la seguridad cibernética también se han vuelto más complejos a medida que el panorama de amenazas continúa evolucionando, los vectores de amenazas se han expandido y las herramientas y métodos de los atacantes utilizados para lanzar agresiones se han vuelto cada vez más sofisticados. El panorama conjunto de amenazas en expansión, los desafíos inherentes a la gestión de la seguridad, las arquitecturas distribuidas e híbridas, la computación en la nube y la necesidad de una conectividad confiable y de alta velocidad para personas y cosas, es el desafío actual de la ciberdefensa.

"Investigación Datos y Computadores IDC Colombia Limitada estima que las empresas a nivel mundial gastan más de $ 100 mil millones en productos y servicios de seguridad para ayudar a protegerse contra las amenazas cibernéticas. Demostrar la efectividad del gasto en ciberseguridad es una prioridad para los ejecutivos corporativos y la junta directiva; sin embargo, cuantificar y justificar el nivel apropiado de gasto sigue siendo un desafío para la mayoría de los equipos de seguridad empresarial. Buscar dólares incrementales para continuar construyendo una postura de seguridad sólida es difícil en el contexto de un mayor número de violaciones cibernéticas que han causado un daño financiero y de reputación significativo a empresas de una variedad de industrias" (Curtis Price et al., 2021).

Así las cosas, el ciberespacio se desenvuelve en un ambiente VICA (volatilidad, incertidumbre, complejidad y ambigüedad), en el que los riesgos y las amenazas se materializan de manera exponencial por su alta masificación, además de la falta de cultura por parte del usuario final, de ahí que se proyecta qué tanto las empresas, la academia y las fuerzas de ley, sigan fortaleciendo la defensa y seguridad a nivel digital para el normal desarrollo de sus operaciones.

Una de las formas para fortalecer esta defensa es a través de las plataformas de simulación y/o juegos de guerra que permiten el entrenamiento y reentrenamiento constante y controlado, y facilitan la toma de decisiones, concientización y sensibilización en distintos escenarios; pero su poco estudio, estandarización, elevado valor comercial dificultan tener una herramienta que se ajuste a las necesidades del país, generando falencias como:

- Estado (bajo) de la capacitación, entrenamiento y reentrenamiento de ciberdefensa a nivel estratégico, táctico y técnico.

- Aumento exponencial de ataques cibernéticos al gobierno y sus instituciones por inexperiencia de algunas instituciones para responder y mitigar ataques de naturaleza cibernética.

- Poco uso de los juegos de guerra para el dominio cibernético por su desconocimiento.

Adicionalmente, sobre los juegos de guerra o simulación en el dominio ciberespacial existe una baja producción científica, sin una definición concreta, ni unos estándares definidos. Por eso surge la necesidad de realizar una revisión de la literatura científica a través de una bibliometría, para poder obtener una posible hoja de ruta que permita definir su importancia en función de las competencias que deben generar y las mejores estrategias para su implementación y evaluación.

Bibliometría

La bibliometría estudia la comunicación escrita desde la producción y difusión, además del desarrollo de las disciplinas, con el fin de realizar pronósticos útiles para la toma de decisiones en los procesos científicos, a través de medidas matemático-aritméticas, técnicas de recuento y análisis (Hernando et al., 2018).

La bibliometría también se entiende como la aplicación del análisis cuantitativo y estadístico de las publicaciones, como artículos de revistas, organizados en las bases o repositorios científicos, por medio de la evaluación cuantitativa de los datos por cada publicación, evaluando el crecimiento, madurez, autores principales, mapas conceptuales e intelectuales y las tendencias de una comunidad científica. La bibliometría también se utiliza en la evaluación del desempeño de la investigación, especialmente en los laboratorios universitarios y gubernamentales, también por los encargados de formular políticas, los directores y administradores de investigación, los especialistas en información y bibliotecarios, y los propios académicos (Granados-León, 2020).

La importancia radica, en qué permite evaluar la ciencia y los científicos, permitiendo identificar los agentes más capacitados de los sistemas científicos y cómo sirve para la correcta asignación de recursos o el establecimiento de prioridades (Torres-Salinas & Jiménez-Contreras, 2012). Además, posibilita la revisión de la literatura para analizar y discutir sobre temáticas asociadas a un medio específico en el universo científico.

La bibliometría se vale de los indicadores bibliométricos para medir principalmente la calidad, producción e impacto. Estos indicadores ofrecen un estándar para la medición del desarrollo científico, aunque algunos críticos insisten en las debilidades como herramientas de evaluación al medir únicamente la producción y el impacto (Prins, 1990). No obstante, los indicadores generan información relevante sobre el proceso de investigación, volumen, evolución, visibilidad, estructura, actividad-producción e influencia, sobre todo permiten a la institucionalidad unificar criterios para las decisiones técnicas, administrativas y políticas (Gallagher & Barnaby, 1998; Hernando et al., 2018).

Juegos de guerra

Los juegos de guerra son una herramienta para explorar las posibilidades de toma de decisiones en un entorno con información incompleta e imperfecta (Mark Herman et al., 2009). El Departamento de Juegos de Guerra – War Gaming Departament – por sus siglas en ingles WGD los define como "un modelo o simulación de guerra cuya operación no involucra las actividades de las fuerzas militares reales, y cuya secuencia de eventos afecta y es, a su vez, afectada por las decisiones tomadas por los jugadores que representan a los bandos opuestos" (Burns et al., 2015).

Sobre los juegos de guerra enfocados a la ciberdefensa, Edward JM Colber, Alexander Kott y Lawrence P Knachel, los definen como muchas formas diferentes de un evento de ejercicio, prueba, simulación o emulación. Por lo general, a diferencia de las pruebas de penetración en las que los piratas informáticos de "sombrero blanco" buscan encontrar las vulnerabilidades técnicas de la empresa, un juego de guerra cibernético corporativo a menudo pone énfasis en un escenario comercial que involucra una sección transversal (Colbert et al., 2020).

Gamificación

Se puede entender como "el uso de la mecánica, la estética y el concepto de los juegos, con el objetivo de proporcionar compromiso entre las personas, motivar acciones, fomentar el aprendizaje y promover la resolución de problemas en escenarios no lúdicos. Para ello, se incorporan sistemáticamente elementos presentes en los juegos a situaciones no lúdicas" (Mendes et al., 2022).

Según Lagares-Galán et al. (2022) un servicio de gamificación sirve para mejorar la cultura de la ciberseguridad. La gamificación es una técnica de aprendizaje que busca trasladar la mecánica de los juegos al ámbito educativo con el fin de mejorar sus resultados.

Ciberdefensa

Capacidad del Estado para prevenir y contrarrestar toda amenaza o incidente de naturaleza cibernética que afecte la sociedad, la soberanía nacional, la independencia, la integridad territorial, el orden constitucional y los intereses nacionales, implica el empleo de las capacidades militares ante amenazas cibernéticas, ataques cibernéticos o ante actos hostiles de naturaleza cibernética (Decreto 338 - Establecer Los Lineamientos Generales Para Fortalecer La Gobernanza de La Seguridad Digital., 2022).

Metodología

Esta investigación por su naturaleza y composición se ubica en un nivel comprensivo, puesto que explica las situaciones que generan el evento. De este modo la investigación está centrada a explicar, predecir y proponer (Barrera, 2012). A manera proyectiva plantea unas líneas de acción desde los juegos de guerra para la ciberdefensa. Para ello se establecieron dos fases principales.

La primera, trató de la revisión de literatura utilizando la metodología de estudios bibliométricos, donde se capturaron los datos a través del metabuscador Scopus. Se sabe que existe otro metabuscador clave que es Web of Science, sin embargo, se utiliza Scopus por ser la mayor base de metadatos bibliográficos que se encuentra en actividad desde el año 2004. Su cobertura de búsqueda cubre más de 5000 casas editoras y más de 1800 revistas indexadas, y su factor de impacto de la actividad científica es de 0,79 sobre 0,17 de Web Science (Juan Manuel Villalobos Álvarez, 2021), lo que la hace de mayor relevancia para el desarrollo de un análisis bibliométrico.

En la segunda fase, se verifica el marco conceptual y estado del arte de los juegos de guerra en ciberdefensa, producto de la primera fase, con el objetivo de caracterizar los diferentes juegos enfocados a la ciberdefensa y cómo estos apoyan en su estrategia, para de ahí saltar al desarrollo de unas posibles líneas de acción que permitan generar próximos estudios de investigación o que sean utilizadas como herramientas en la gestión de la ciberdefensa a través de la utilización de estos juegos.

Resultados

Procedimiento de búsqueda, captura y procesamiento de información

Los documentos analizados fueron capturados en el metabuscador Scopus, siendo la fecha de corte de la búsqueda el día 01 de junio de 2022. Los criterios de búsqueda, sentencia de búsqueda, se enfocaron en la unión de las palabras clave del tema: ciberdefensa, ciberseguridad y juegos de guerra; utilizando las diferentes variaciones y palabras clave relacionadas, en un ejercicio de prueba y error, para encontrar los resultados más significativos. El motor de búsqueda fue el siguiente:

(TITLE (wargame) OR TITLE (wargaming) OR TITLE (war AND game) OR TITLE (war AND gamming) OR TITLE (war-game) OR TITLE (war-gaming) OR TITLE (war-simulation) OR TITLE (war AND simulation) OR TITLE (military AND game) OR TITLE (military AND gaming) OR TITLE (military AND simulation) OR TITLE (naval AND game) OR TITLE (navy AND game) OR TITLE (naval AND gaming) OR TITLE (navy AND gaming) OR TITLE (warfaregame) OR TITLE (warfaregaming) OR TITLE (warfare AND game) OR TITLE (warfare AND gaming) OR TITLE (warfare AND simulation) OR TITLE (warfare-game) OR TITLE (warfare-gaming) OR TITLE (warfare-simulation) OR TITLE (cyberdefense AND game) OR TITLE (cyberdefense AND gaming) OR TITLE (cyber-defense AND game) OR TITLE (cyber-defense AND gaming) OR TITLE (cyber AND defense AND game) OR TITLE (cyber AND defense AND gaming) OR TITLE (army AND game) OR TITLE (army AND gaming) OR TITLE (army AND simulation) OR TITLE (air AND force AND game) OR TITLE (air AND force AND gaming) OR TITLE (air AND force AND simulation) OR TITLE (national AND defense AND game) OR TITLE (cyberdefence AND game) OR TITLE (cyber AND defence AND game) OR TITLE (cyberdefence AND gaming) OR TITLE (cyber AND defence AND gaming)).

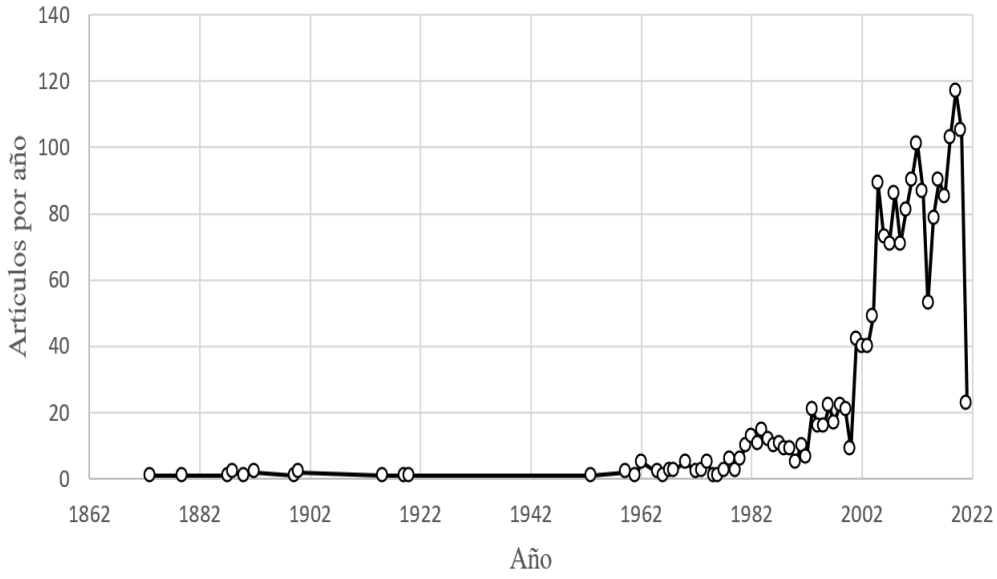
Se encontraron 1908 documentos entre artículos, libros, documentos de sesión, entre otros desde el año 1873, ya que este es el año donde se arroja el primer documento sobre el tema en esta base de datos, hasta el año 2022. Posteriormente, se procedió a realizar el análisis estadístico por medio del programa R Project for Statistical Computing, implementando el paquete «bibliometrix».

Resultados de índices e indicadores bibliométricos

Producción en el tiempo

El análisis de la línea de tiempo entre los años 1873 y 2022 de los documentos, evidencia que, de los 1908 documentos existentes sobre el tema, 426 de estos (Figura 1) correspondientes al 42,85%, fueron escritos en los años 2012, 2018 a 2022 (Figura 2); el porcentaje de crecimiento anual del 2.14%, permite evidenciar el limitado interés que el tema está teniendo en la actualidad a nivel científico, observando así un registro de 3918 autores que publicaron en revistas, documentos de conferencia, libros, etc., con un promedio de 4272 citas por documento y 7594 palabras claves mostradas.

Figura 1.
Producción de documentos por año



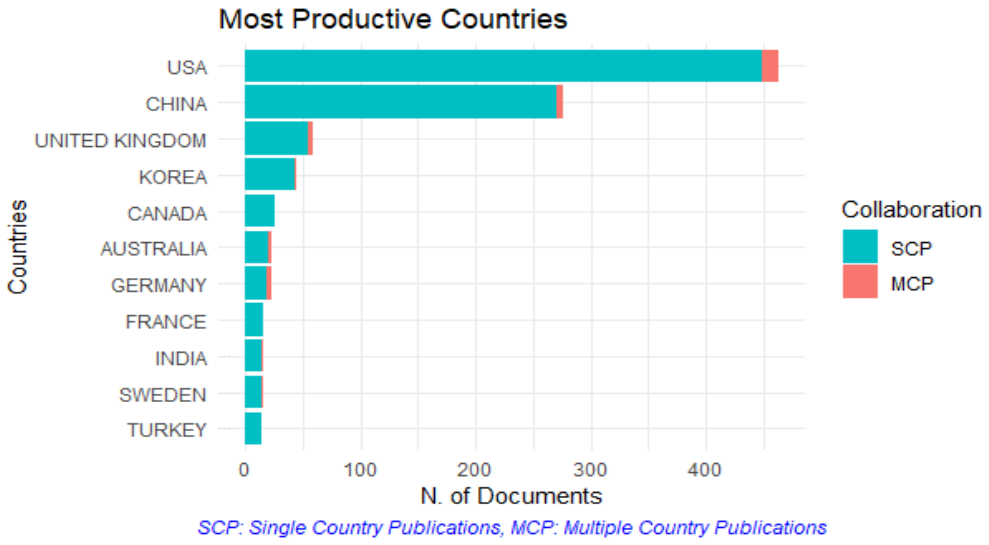
Fuente: Elaboración propia usando Bibliometrix.

Figura 2.
Porcentaje producción de documentos de la muestra por año

Fuente: Elaboración propia usando Bibliometrix.

El país más productivo en cuanto al tema es Estados Unidos, con una producción de 463 artículos, seguido de China (276) y de otros países como Reino Unido, Corea y Canadá (Figura 3).

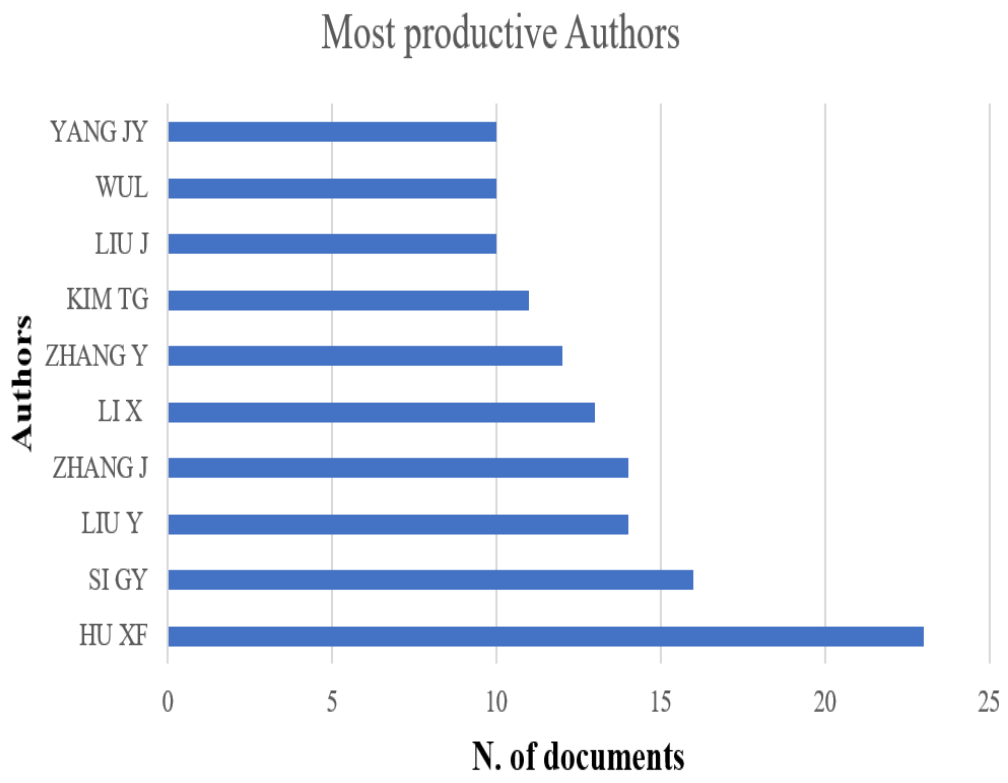
Figura 3.
Países más productivos



Fuente: Elaboración propia usando Bibliometrix.

Los 10 autores más productivos son Hu XF (23), Si GY (16), Liu Y (14), Zhang J (14), Li X (13), Zhang Y (12), Kim TG (11), Liu J (10), Wul (10) y Yang J (10) cómo se muestra en la Figura 4.

Figura 4.
Autores más productivos



Fuente: Elaboración propia usando Bibliometrix.

Las principales publicaciones académicas de la muestra fueron por parte de Xitong Fangzhen Xuebao / Journal Of System Simulation (112), Proceedings Of Spie - The International Society For Optical Engineering (70), Winter Simulation Conference Proceedings (61), Lecture Notes In Computer Science(37), Proceedings - Winter Simulation Conference (34), Simulation Series (18), Xi Tong Gong Cheng Yu Dian Zi Ji Shu/Systems Engineering And Electronics (18), Journal Of Defense Modeling And Simulation (15), Military Medicine (15) y Sae Technical Papers(15). Esto muestra que las revistas de simulación y las actas de conferencia son los documentos mayormente citados en relación con el campo de estudio y son los que contribuyen a la base investigativa en el tema de juegos de guerra.

Índice h, g y m de los autores.

El índice "h" hace referencia a un indicador de impacto, donde se mide el número de investigaciones publicadas por un autor y las citas que se han obtenido de

este, demostrando una relación entre el índice y el éxito del investigador. Entonces, un número "h" de publicaciones, han recibido un número mínimo "h" de citas (Túñez López & de Pablos Coello, 2013).

El índice "g" por su parte, realiza el cálculo sobre la productividad científica determinada por el historial de publicaciones de los autores. Para obtener este cálculo son listadas las publicaciones de un autor en orden descendente de acuerdo con el número de citas recibidas por cada uno de ellos y luego este digito se eleva al cuadrado (Túñez López & de Pablos Coello, 2013).

Finalmente, el índice "m" se calcula a través de la relación h/n, siendo n el número de años de carrera como investigador, lo cual representa la mediana de las citas recibidas por el índice "h" (Moral Muñoz et al., 2019).

Para el caso particular, los autores con mayor índice h (4) son Si GY, Liu Y, Kim TG y Yang JY; de la misma forma, se evidencia que el autor con mejor índice g (10) es Liu Y; por otra parte, el autor con mejor índice m es Kim TG (0,23), lo que muestra que este último publica artículos más frecuentemente que los demás autores (Tabla 1).

Tabla 1.
Índice h, g y m de los primeros 10 autores

Autor	Índice H	Índice G	Índice M
Hu XF	4	5	0.19
Si GY	3	4	0.14
Liu Y	4	10	0.19
Zhang J	3	4	0.15
Li X	2	2	0.11
Zhang Y	3	8	0.15
Kim TG	4	6	0.23
Liu J	2	2	0.12
Wu L	3	4	0.15
Yang JY	4	5	0.21

Fuente: Elaboración propia.

Ranking de dominancia de los autores.

El factor de dominancia es el que determina el número de artículos de varios autores en los que aparece un investigador, considerado erudito en el tema, como primer autor en las publicaciones (Elango & Rajendran, 2012). Según lo encontrado en el análisis, Zhang J y Li X son los de más alto nivel de dominancia, ya que, de 14 y 13 artículos publicados, los dos aparecen como primer autor en 5 de estos; los segundos son Liu J y Zhang Y debido a que,

de 10 y 12 artículos publicados, aparecen en 4 como primer autor. Los demás autores pueden verse en la Tabla 2.

Tabla 2.
Ranking de dominancia de los autores.

Autor	Factor de dominancia	Total, de artículos	Un solo autor	Múltiples autores	Primer autor
Liu J	0.4	10	0	10	4
Zhang J	0.38461538	14	1	13	5
Li X	0.38461538	13	0	13	5
Zhang Y	0.33333333	12	0	12	4
Yang JY	0.3	10	0	10	3
Si GY	0.1875000	16	0	16	3
Hu XF	0.14285714	23	2	21	3
Liu Y	0.14285714	14	0	14	2
Wu L	0.1	10	0	10	1
Kim TG	0.09090909	11	0	11	1

Fuente: Elaboración propia.

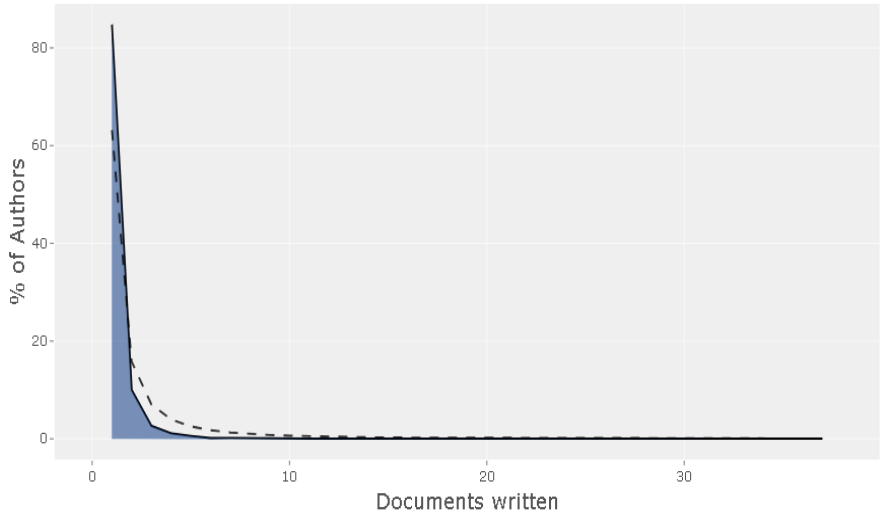
Estimación del Coeficiente de la Ley de Lotka

La Ley de Lotka describe la distribución productiva de los autores y las contribuciones producidas en un campo dado a lo largo de un periodo de tiempo, donde se distingue que la producción científica del tema se centra en un número determinado de autores que publican un mayor número de artículos (Elango & Rajendran, 2012; Urbizagástegui Alvarado, 1999).

Aplicando la Ley de Lotka (Figura 5), se observa que existen 3321 autores que han escrito un solo artículo sobre el tema de juegos de guerra. El total de autores que han escrito dos artículos son 393; tres artículos, 105; cuatro artículos, 44; cinco artículos, 23; seis artículos, 6; siete artículos, 7; ocho artículos, 4; nueve artículos, 3 y diez artículos, 4.

Al comparar la estimación teórica de la Ley de Lotka y el comportamiento de la muestra estudiada, se espera que no haya diferencias significativas entre las dos muestras.

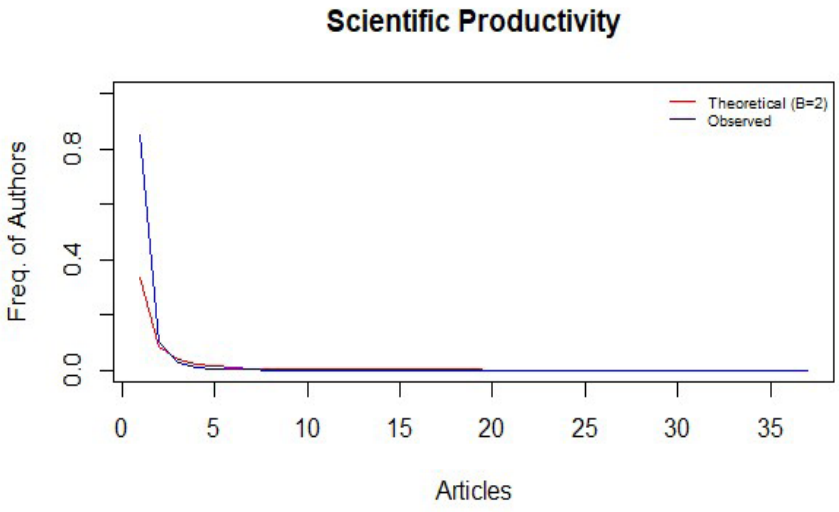
Figura 5.
Estimación coeficiente Ley de Lotka



Fuente: Elaboración propia usando Bibliometrix.

El coeficiente Beta estimado es 2.53, constante 0.33 con una bondad de ajuste igual a 0.90. La prueba de dos muestras de Kolmogorov-Smirnoff proporciona un valor de p = 0.04, lo que quiere decir que sí existe una diferencia significativa entre las distribuciones Lotka observadas y las teóricas (Figura 6).

Figura 6.
Comparación de la beta teórica con la observada de las distribuciones Lotka



Fuente: Elaboración propia usando Bibliometrix.

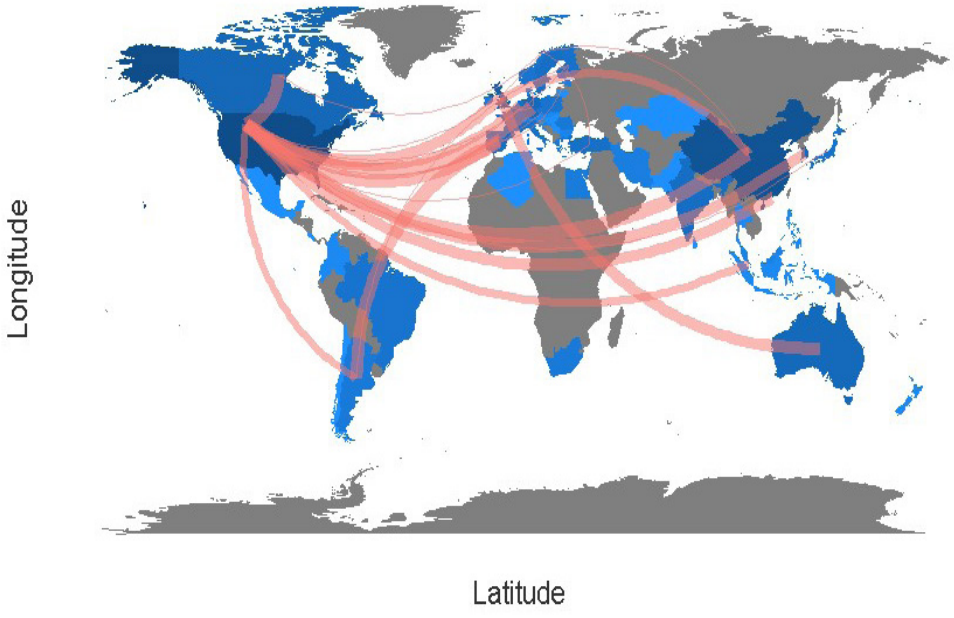
Acoplamiento Bibliográfico

Dos artículos están acoplados bibliográficamente si al menos una fuente citada se encuentra en la lista de referencias de dos artículos. La fuerza del acoplamiento de los dos artículos se calcula a partir del número de referencias compartidas en común por estos mismos, además de introducir el acoplamiento entre la co-cita, la co-ocurrencia de palabras clave y la cooperación entre países (Aria & Cuccurullo, 2017).

Colaboración Científica Internacional

Una red de colaboración científica es aquella que se estimula por medio de políticas de promoción de la investigación mediante la financiación y tienen como objetivo la cooperación internacional para generar producción científica (Sá Carvalho, Travasso y Medina, 2014). Es aquí donde se observa que los nodos son autores y los enlaces son coautorías entre estos. Si el nodo es de mayor tamaño, quiere decir que hay más cantidad de autores de ese país en coautoría con otros. En el caso del presente análisis, se evidencia que el país que más cooperación de coautorías tiene en relación con el tema de juegos de guerra es Estados Unidos, que está unido a 8 países, destacando sus conexiones con Francia, Canadá, China, Japón y Corea; así mismo. China está unido con 4 países, siendo estos Reino Unido, Alemania, Australia y Dinamarca (Figura 7).

Figura 7.
Colaboración científica internacional.

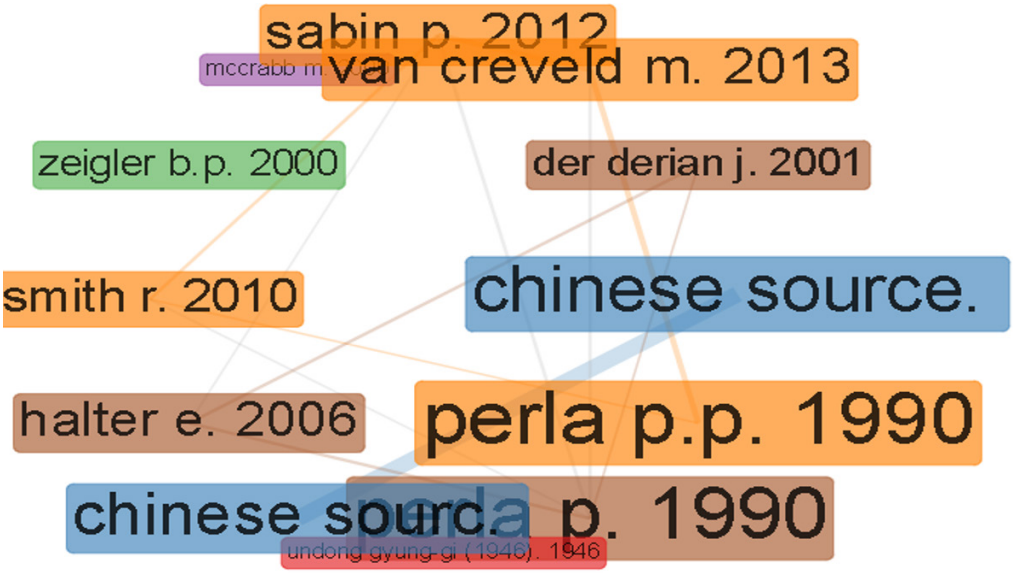


Fuente: Elaboración propia usando Bibliometrix.

Red de Co-citas

La red de co-citación observa cuando ambos artículos son citados en un tercer artículo (Aria & Cuccurullo, 2017). En la figura 8 se muestra el nodo de artículos de autores eruditos, siendo para este caso los artículos de Perla (1990) y los de la Revista China los que evidencian un nodo más grande y están espacialmente más cerca entre sí, en comparación con otros artículos menos populares como los de Der Derian (2001) y Sabin (2012).

Figura 8.
Red de co-citación.

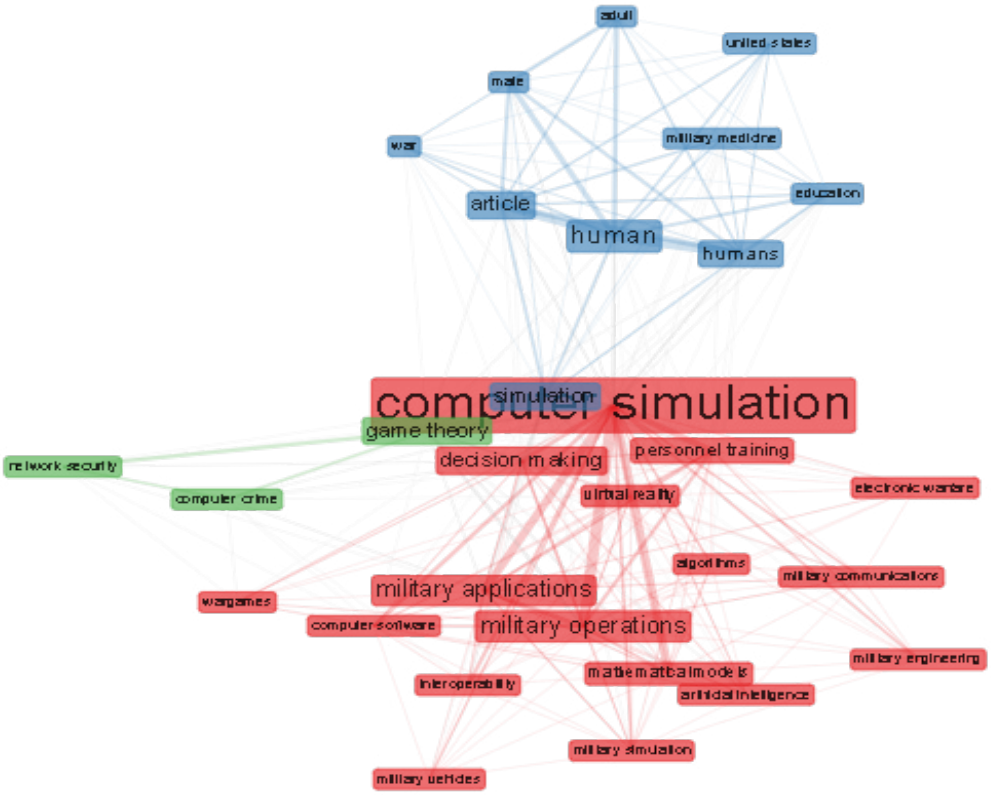


Fuente: Elaboración propia usando Bibliometrix.

Red de Coocurrencia de palabras clave

La Figura 9 muestra tres conglomerados de nodos claramente divididos: uno en color rojo encabezado por las palabras "simulación informática", acompañado de otras palabras menos concurrentes como aplicaciones militares, toma de decisiones, operaciones militares, inteligencia artificial y juegos de guerra. El otro nodo, mostrado en color azul, está encabezado por las palabras "simulación" y "humano", acompañado de palabras como educación, medicina militar, humanos, adultos, guerra, artículo, Estados Unidos y masculino. Por último, se puede observar un nodo de color verde, en el cual se encuentran palabras compuestas como seguridad de la red, crimen informático y teoría de juego. Se puede afirmar que uno de los nodos muestra cuál es el contexto de investigación general del tema de juegos de guerra (nodo rojo), mientras que el otro nodo muestra el modo de estudio y aplicación del concepto (azul) y el nodo de color verde muestra temas emergentes en este tipo de investigaciones.

Figura 9.
Co-ocurrencias de palabra clave.

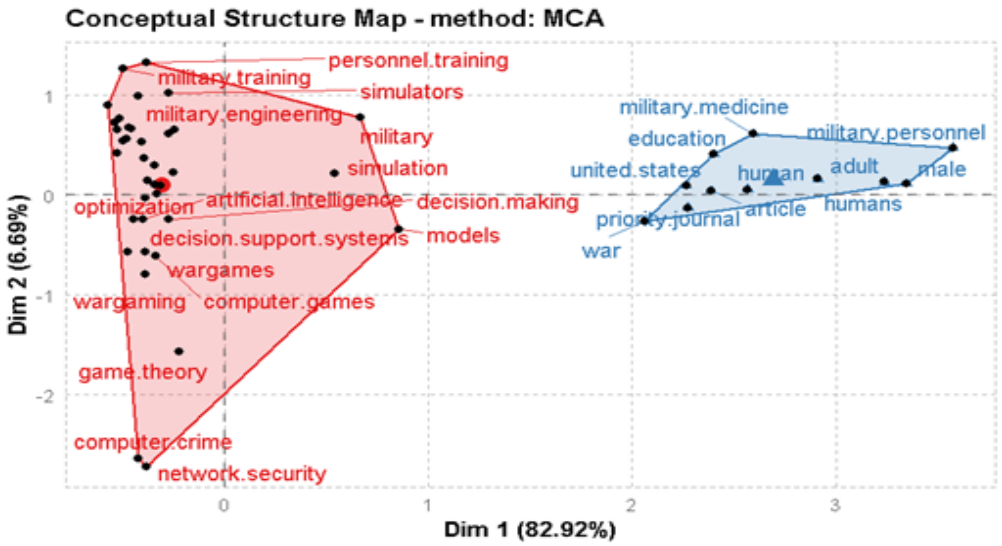


Fuente: Elaboración propia usando Bibliometrix.

Áreas de investigación.

Se muestran las áreas de investigación que están relacionadas en torno al tema juegos de guerra a través de un análisis de correspondencias múltiples (ACM), el cual analiza la homogeneidad de la matriz de indicadores para obtener una representación euclidiana de baja dimensión de los datos originales (Abdi y Valentin, 2007). En el presente caso, la Figura 10 muestra dos grandes campos de investigación principales, esto se logró al mapear las co-ocurrencias de palabras en la colección bibliográfica. En el campo rojo se observan investigaciones relacionadas con entrenamiento militar, entrenamiento de personal, simulación militar, inteligencia artificial, toma de decisiones, crimen informático, juego de guerra, entre otros; y en el campo azul se muestran estudios de educación, medicina militar, entrenamiento militar, Estados Unidos, humanos, etc.

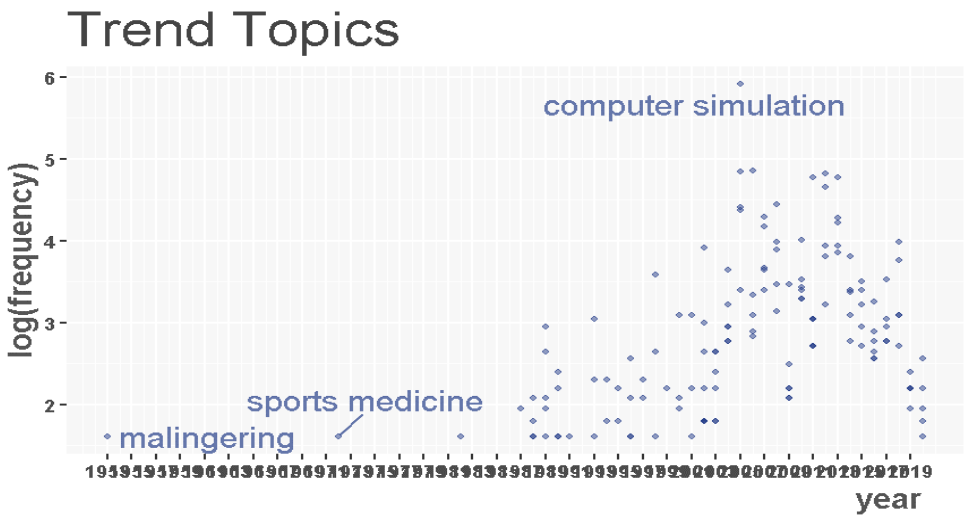
Figura 10.
Estructura conceptual del campo de ideología religiosa.



Fuente: Elaboración propia usando Bibliometrix.

Finalmente, en la Figura 11 se observa la tendencia temática a lo largo de los últimos años, la cual se centra en simulación informática, medicina deportiva y simulación.

Figura 11.
Dendrograma temático



Fuente: Elaboración propia usando Bibliometrix.

Discusión

El estudio bibliométrico de los juegos de guerra en ciberseguridad y ciberdefensa muestra que la investigación, desarrollo y producción de ciencia e innovación es impulsada por países asiáticos y norteamericanos, quienes priorizan este tipo de temas para el desarrollo de capacidades en ambientes controlados para "aprender jugando", así como la toma de decisiones en los niveles, estratégicos, tácticos y técnicos, y la sensibilización y concientización de las personas (Cano M, 2019), teniendo en cuenta la relevancia del ciberespacio como capacidad estratégica de cada nación.

Algo diferente pasa en países latinoamericanos, donde es escasa la producción científica en juegos de guerra. Esto podría ser por la falta de incentivos para ejercer, la consecución de recursos, el acceso a bibliografía en lengua nativa, el desconocimiento del tema y por la ausencia de políticas de estado robustas que pongan como una prioridad el ciberespacio.

Los juegos de guerra son una tendencia y prioridad creciente en el área de la simulación computacional para la toma de decisiones, requiriendo de ambientes controlados que permitan el desarrollo de técnicas, tácticas y procedimientos para el mejoramiento continuo de la ciberseguridad, ciberdefensa y ciberinteligencia. Sin embargo, los juegos de guerra no son exclusivos para la ciberseguridad, son utilizados también en ciencias militares, deportes, medicina, entre otros. De ahí la importancia de realizar una caracterización de los tipos de juegos de guerra que se aplican actualmente en ciberdefensa y ciberseguridad como apoyo a la gestión estratégica.

"Los juegos de guerra adquieren importancia por la necesidad de probar y experimentar con entornos cercanos a la realidad, sobre esto la revista del Army Cyber Institute, "Wargaming and the education GAP" menciona:

> "Los juegos de guerra se han convertido en un método para formular, promulgar y analizar cursos de acción en búsqueda de un objetivo específico, ya sean operaciones cinéticas militares, esfuerzos de socorro en casos de emergencia y desastres o escenarios del fin del mundo. Un objetivo deseado de los juegos de guerra es el análisis asociado, porque es el medio para cuantificar los datos de los resultados de los juegos de guerra con fines operativos. El punto en común entre la mayoría de los eventos de juegos de guerra de mapas y modelos es que se ocupan principalmente del dominio físico. Un evento que es táctil y físicamente observable por naturaleza, donde las reglas están claramente definidas como el tiempo, los recursos, las ubicaciones, las distancias y la secuencia de acciones. El juego de guerra en el dominio físico es bien entendido y practicado, pero ¿cómo podemos jugar en el dominio cibernético?" (Long, 2020).

Es de mostrar que los juegos de guerra en el ámbito cibernético no son relativamente nuevos. En 1983 se lanza a la pantalla grande la película "Juegos de Guerra" dirigida por John Badham, en la que un joven hacker descubre un ordenador vulnerable del Departamento de Defensa de los Estados Unidos, utilizando una técnica de marcado de números al azar con su módem, y desde su ordenador toma control de los silos nucleares. La trama de esta película generó que el presidente del momento de los Estados Unidos, Ronald Reagan preguntara

si algo como esto podría suceder, a lo que la Agencia Nacional de Seguridad (NSA) respondió: "la situación es mucho peor de los que usted pueda imaginar" (ALVY, 2016), subrayando el ciberespacio, sus riesgos y vulnerabilidades como una amenaza real para los Estados Unidos. Se podría decir que ante estos acontecimientos se empieza a dar un grado de importancia y desarrollar los juegos de guerra cibernéticos, tal como lo pudimos corroborar en el estudio bibliométrico desarrollado.

Tipos de Juegos de Guerra

Se puede dividir los juegos de guerra cibernéticos en tres grupos:

- Estratégico
- Técnico
- Táctico

En la parte estratégica encontramos juegos de guerra enfocados a los tomadores de decisiones, y son juegos por lo regular temáticos, con casos, ejemplos, lecciones aprendidas y situaciones posiblemente reales de amenazas, riesgos o ataques en el ciberespacio y con una afectación al Estado, infraestructura crítica (Guarda et al., 2017).

Figura 12.
División de los juegos de Guerra ciber según su nivel

Fuente: Elaboración propia.

Para el entrenamiento, reentrenamiento, sensibilización en todos los niveles son comunes los siguientes tipos de ejercicios:

Tabletop Exercise

Los ejercicios de mesa o más conocidos por su anglicismo "Tabletop Exercise - TTE", los cuales según la "National Institute of Standards and Technology", por sus siglas en inglés (NIST), son ejercicios basados en debates en los que el personal se reúne en un salón o en grupos para analizar sus funciones durante una emergencia y sus respuestas ante una situación de emergencia en particular. Un facilitador presenta un escenario y hace preguntas a los participantes del ejercicio relacionadas con el escenario, lo que inicia una discusión entre los participantes sobre roles, responsabilidades, coordinación y toma de decisiones. En general son ejercicios de simulación basados únicamente en debates y no implica el despliegue de equipos u otros recursos (Grance et al., 2002), por lo que son excelentes ejercicios para los niveles gerenciales y de toma de decisiones, ya que no tienen un componente técnico complejo y por el contrario se basan en escenario reales o irreales del mundo ciber.

Juegos de roles o de confrontación

El juego de roles es una técnica de grupo ampliamente utilizada en formación que se dirige, fundamentalmente, al entrenamiento en habilidades sociales y de comunicación. El juego de roles consiste en la representación de papeles (roles), por parte de uno o más individuos. Estos roles se definen de manera que se apliquen determinadas habilidades, aquellas que se pretende establecer y mejorar. Los juegos de roles generalmente tienen tres tipos de participantes: jugadores, observadores y facilitadores (Alteco, 2022).

Este es un método riguroso que descompone los conflictos en dilemas identificables. Estos dilemas se clasifican en persuasión, confianza, rechazo, cooperación y amenaza. El método entonces ayuda a resolver problemas. Este método es útil cuando se trata de resolver confrontaciones entre estados nacionales que podrían conducir a un conflicto cibernético. También puede ayudar a prevenir la escalada cibernética (Curry & Drage, 2018).

Lego Serious Play

Una poderosa herramienta diseñada para potenciar la innovación y el rendimiento; son los LEGO® SERIOUS PLAY®, que son un proceso de encuentro, comunicación y resolución de problemas en el que los participantes son guiados a través de una serie de preguntas para sondear cada vez más profundo sobre el tema. Cada participante construye su propio modelo 3D LEGO® en respuesta a las preguntas del facilitador, utilizando elementos LEGO® especialmente seleccionados. Estos modelos 3D sirven como base para la discusión en grupo, el intercambio de conocimientos, la resolución de problemas y toma de decisiones. (Garzón & Garzón, 2020). Este método puede respaldar, mejorar y fortalecer el diseño, la ejecución y los resultados de los Ejercicios de mesa que se utiliza para evaluar las capacidades, la eficacia y la madurez de los equipos de Ciberseguridad, los CSIRT[4].

4 Decreto 338 del 8 marzo del 2022 define CSIRT como: (Computer Security Incident & Response Team) Equipo de Respuesta a Incidentes de Seguridad Cibernética, por su sigla en inglés. Es el equipo que provee las capacidades de gestión de incidentes a una organización/sector en especial. Esta capacidad permitir minimizar.

Capture the Flag

Para técnicos y tácticos por lo regular se utilizan los juegos que fortalezcan y refuercen los conceptos, así como entrenar y reentrenar al personal que ejerce las funciones de ciberseguridad, esto por medio de pruebas con diferentes niveles de dificultad, como es el caso del juego "Captura la Bandera", pero más conocido en el argot técnico por su anglicismo "Capture the Flag" o CTF.

Un CTF es un tipo de competición perteneciente al mundo de la seguridad digital, que consiste en resolver una prueba o desafío informático con el fin de encontrar la bandera que, en este caso, representa la solución. Este enfoque pedagógico consigue que los usuarios tengan que demostrar conocimientos específicos, investigar todas las posibilidades ante un problema, desarrollar un proceso de estudio y elegir el camino más adecuado para encontrar la solución. (Sancho Núñez et al., 2021).

Dentro de los juegos de Capture the Flag existen diferentes tipologías como, Jeopardy, Attack-Defense, o mixto, siendo este último la combinación de los anteriores. Además, estos juegos se pueden orientar a diferentes disciplinas o retos, para entrenar, capacitar o medir las habilidades de los participantes, por ejemplo, recolectar información utilizando técnicas de Open Source Intelligent (OSINT), análisis forense, criptografía, esteganografía, explotación, ingeniería inversa, programación, explotación web, reconocimiento, trivias, o misceláneo (Sancho Núñez et al., 2021).

Cyber Range

Una de las expresiones que resaltan en el estudio bibliométrico y que sirven para el apoyo en la simulación de juegos de guerra cibernéticos, es el concepto relativamente nuevo de Cyber Range, que define Ishaani Priyadarshini como:

> "Una plataforma virtual que permite simular entornos operativos reales estáticos o desplegables, clasificados o no clasificados para la formación y el entrenamiento individual o colectivo de profesionales, así como la experimentación, el testeo y la validación de nuevos conceptos, tecnologías, técnicas y tácticas de ciberseguridad y ciberdefensa. Es una capacidad estratégica que posibilita que gobiernos y empresas puedan formar y entrenar de manera efectiva a sus profesionales, así como experimentar, testear y validar nuevos conceptos, tecnologías, técnicas y tácticas de ciberseguridad y ciberdefensa"(Priyadarshini & Barner, 2018).

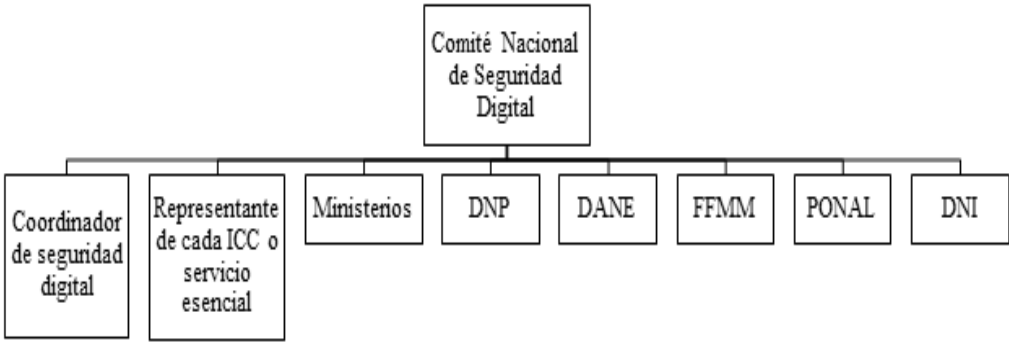
Esta es una herramienta utilizada en ambientes militares, pero que cualquier CISRT debería tener en sus capacidades.

Líneas de acción propuestas

Colombia ha venido desarrollando capacidades en el ámbito ciber y trabajando en el fortalecimiento de la gobernanza digital desde lo público y privado, además, apoyándose en sus FFMM se realizaron las mesas de infraestructuras criticas cibernéticas (ICC) y el Plan Nacional de protección de ICC. Otro de los logros fue el Modelo de Gestión de Riesgos de Seguridad Digital por parte del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC). Otra normatividad

que permitió generar la hoja de ruta y el entorno de ciberdefensa y ciberseguridad en Colombia fueron los CONPES 3701 del 2011, 3854 del 2016 y 3995 del 2021, y más recientemente el decreto 338 del 8 de marzo del 2022 cuyo fin fue "establecer los lineamientos generales para fortalecer la gobernanza de la seguridad digital, la identificación de infraestructuras críticas cibernéticas y servicios esenciales, la gestión de riesgos y la respuesta a incidentes de seguridad digital" (Decreto 338 - Establecer Los Lineamientos Generales Para Fortalecer La Gobernanza de La Seguridad Digital, Se Crea El Modelo y Las instancias de Gobernanza de Seguridad Digital y Se Dictan Otras Disposiciones, pág. 4,2022) y cuya relevancia radica en la definición que hace del Comité de Seguridad Digital (Figura 13) quien tiene la tarea de la coordinación, colaboración y cooperación entre las múltiples partes interesadas, los niveles de la gobernanza digital y el fortalecimiento del entorno digital.

Figura 13.
Gobernanza Digital – Comité de seguridad Digital.

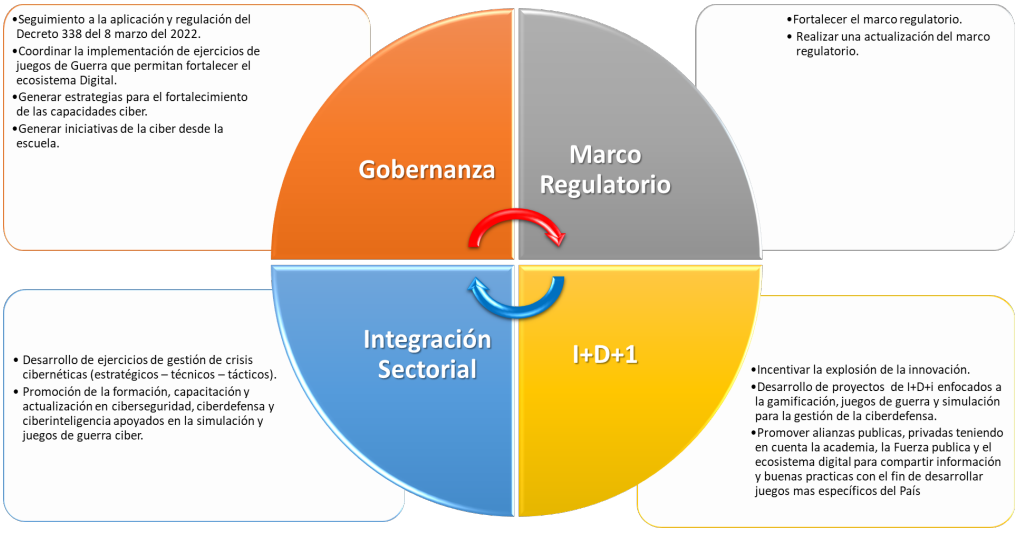


Fuente: Decreto 338 del 8 de marzo de 2022.

El recorrido normativo y de gestión del gobierno colombiano permite que iniciativas de mejora del proceso de toma de decisiones enfocadas en los juegos de guerra tengan éxito. Este es el caso del Ejercicio de Gestión de Crisis Cibernética Nacional realizado y liderado desde el año 2017 por el Comando Conjunto Cibernético (CCOCI) junto con la Escuela Superior de Guerra, que trata de un ejercicio de mesa tipo Tabletop Exercise, donde se invitan a los líderes con capacidad de decisión de los sectores definidos como infraestructuras críticas cibernéticas, personal de los ministerios y Fuerza Pública, para simular un ataque y ver las posibles acciones a desarrollar, y al final del mismo sacar unas conclusiones que permitan retroalimentar a los participantes y ajustar procesos y procedimientos nacionales ante amenazas que impacten las ICC.

Para para garantizar la incorporación de los juegos de guerra cibernéticos en la gestión de la ciberdefensa en Colombia, a continuación, se proponen cuatro líneas de acción (Figura 14):

Figura 14.
Líneas de acción



Fuente: Elaboración propia.

Estas líneas de acción son codependientes y deben desarrollarse de forma paralela, teniendo como hoja de ruta la I+ D+i para la generación de capacidades propias y desarrollar las mejores técnicas, tácticas y procedimientos, utilizando como eje central los juegos de guerra como una herramienta para la concientización de la ciberseguridad y la ciberdefensa del país.

Conclusiones

Se evidencia una carencia de investigaciones relacionadas con los juegos de guerra, esto podría ser por la falta de incentivos para el desarrollo de productos científicos, la brecha del idioma que impide tanto la consulta, como la generación, y el desconocimiento de las bondades de los juegos de guerra para la toma de decisiones.

A pesar de los grandes esfuerzos del país para potencializar la adecuada educación y entrenamiento e I + D + i en materia de ciberdefensa y ciberseguridad, hoy existen importantes carencias marcadas entre otras por la falta de investigación a nivel nacional e internacional en los temas de juegos de guerra ciber. La producción se enfoca en lo cinético y técnico que no enriquece la parte estratégica, dejando a un lado herramientas como los juegos de guerra ciber que pueden apoyar la gestión estratégica de la ciberseguridad y ciberdefensa.

Los juegos de guerra cibernéticos pueden convertirse en la mejor herramienta para todos los niveles de la gobernanza digital, sin embargo, a nivel país no son comunes estas herramientas de apoyo a la toma de decisiones, ya sea por sus costos o por creer que es una responsabilidad sólo de las FFMM.

Se carece de una estrategia en ciberdefensa que permita tener una sinergia operacional y sectorial para la protección de las Infraestructuras Críticas Cibernéticas Nacionales. Esta sinergia puede darse a través de estos juegos, como herramienta para la toma de decisiones, para reducir las dificultades a la hora de comprender la naturaleza interdisciplinar de la ciberseguridad, dado por la falta de entornos de formación colaborativos y coherentes con el espacio de operaciones real.

No se tiene una definición y caracterización estándar de los juegos de guerra en el ámbito cibernético que permita comparar cuáles son los mejores para cada uno de los niveles, siendo esta una oportunidad de investigación y estandarización.

Referencias

Abdi, H. y Valentín, D. (2007). *Multiple Correspondence Analysis. Texas:* Encyclopedia of Measurement and Statistics.

Alteco, consultores. (s/f). Juego de Roles como Técnica de Formación -. Recuperado el 12 de septiembre de 2022, a partir de https://www.aiteco.com/juego de-roles/ALVY. (2016, febrero 23). La influencia de «Juegos de guerra» en la ciberseguridad del MundoRealTM. https://www.microsiervos.com archivo/seguridad/influencia-juegos-de-guerra-mundo-real.html

Aria, M., & Cuccurullo, C. (2017). bibliometrix: An R-tool for comprehensive science mapping analysis. Journal of Informetrics, 11(4), 959–975. https:/ doi.org/10.1016/J.JOI.2017.08.007

Barrera, J. H. (2012). *Proyecto de Investigación comprensión Holística de la Metodología y la Investigación. Caracas:* Ediciones Quirón. Burns, S., della Volpe, D., Babb, R., Miller, N., & Muir, G. (2015). War Gamers Handbook: A Guide for Professional War Gamers. https://apps dtic.mil/sti/citations/AD1001766

Cano M, J. J. (2019). The Human Factor in Information Security. ISACA. www isaca.org

Colbert, E. J. M., Kott, A., & Knachel, L. P. (2020). The game-theoretic model and experimental investigation of cyber wargaming. Journal of Defense Modeling and Simulation, 17(1), 21–38. https://doi org/10.1177/1548512918795061

Curry, J., & Drage, N. (2018, septiembre 10). *Developments in state level cyber wargaming. ACM International Conference Proceeding Series.* https:/ doi.org/10.1145/3264437.3264468

Curtis Price, Christina Richmond, *Craig Robinson, & Philip D. Harris. (2021, abril 25). Ataque de brecha y simulación_ una herramienta fundamental para probar la eficacia de los controles de seguridad* - IDC COLOMBIA Analiza el futuro. http://www.idccolombia.com.co/ataque-de-brecha y-simulacion-una-herramienta-fundamental-para-probar-la-eficacia-de los-controles-de-seguridad/

Elango, B., & Rajendran, P. (2012). *Authorship Trends and Collaboration Pattern in the Marine Sciences Literature: A Scientometric Study. Undefined* https://www.microsiervos.com/archivo/seguridad/influencia-juegos-de guerra-mundo-real.html

Elango, B. y Rajendran, P. (2012). *Authorship Trends and Collaboration Pattern in the Marine Sciences Literature:* A Scientometric Study. International Journal of Information Dissemination and Technology, 2(3), 166-169.

Gallagher, *E. J., & Barnaby, D. P. (1998). Evidence of methodologic bias in the derivation of the Science Citation Index impact factor.* Annals of Emergency Medicine, 31, 83–86. https://doi.org/10.1016/S0196-0644(98)70286-0

Garzón, F., & Garzón, G. (2020). *Cybersecurity Incident Response Tabletop Exercises Using the Lego Serious Play Method.* https://www.isaca.org resources/isaca-journal/issues/2020/volume-4/cybersecurity-incident response

Granados-León, C. (2020). Bibliometría: *Una tendencia en la investigación en marketing. Working Papers. Maestría En Gerencia Estratégica de Mercadeo, 1(4)*. https://doi.org/10.15765/wpmgem.v1i4.1475

Grance, T., Nolan, T., Burke, K., Dudley, R., White, G., & Good, T. (2002) *Special Publication 800-84 Sponsored by the Department of Homeland Security Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities Recommendations of the National Institute of Standards and Technology*. https://doi.org/10.6028/NIST.SP.800-84

Guarda, T., Vaca, O. B., Pinguave, M. P., *Maldonado, E. P., Augusto, M. F., Orozco, W., & Pinto, F. M. (2017). Wargames applied to naval decision making process.* Advances in Intelligent Systems and Computing, 571, 399–406. https://doi.org/10.1007/978-3-319-56541-5_41

Gutiérrez-Salcedo, M., Martínez, M. Á., *Moral-Muñoz, J. A., Herrera-Viedma, E., y Cobo, M. J. (2018). Some bibliometric procedures for analyzing and evaluating research fields.* Applied intelligence, 48(5), 1275-1287.

Hernando, J., *Stephany, Á.-T., Eugenio, V., Guajardo, S., Castro, A., Yuly, R., Colorado, S., Pérez-Anaya, O., Daniela, A., Ivón, M.-E., Alexander, R.-P., Alexander, P.-R., Noelia, M.-M., María, J.-F., & Oregioni, S. (2018). Cienciometría y bibliometría. El estudio de la producción científica Métodos, enfoques y aplicaciones en el estudio de las Ciencias Sociales Autores* (Primera Edición). www.unireformada.edu.co

Juan Manuel Villalobos Álvarez. (2021). *Análisis bibliométrico años 2000-2021: modelamiento y simulación en ciberseguridad y ciberdefensa. Revista Derotero, 1, 77–102.* https://www.escuelanaval.edu.co/es/revistaderrotero

Lagares-Galán, J., Navas-Pérez, P. J., *Peregrina-Pérez, M. J., & Boubeta-Puig, J. (2022). Un Servicio de Gamificación para Mejorar la Cultura de la Ciberseguridad *.* Universidad de Cadiz, 10.

Long, D. T. (2020). Wargaming and the Education Gap. The Cyber Defense Review, 5(1), 185–200. https://www.jstor.org/stable/26902670

Mark Herman, Mark Frost, & Robert Kurz. (2009). Consejos Guerra Líderes Toma De Decisiones Estratégicas Desde El Campo De Batalla. 275.

Mendes, D. de S., Lima, M. R. de, & Freitas, T. A. R. de. (2022). *Gamificación, "no tengo ni idea de lo que es": un estudio en la Formación Inicial del Profesorado de Educación Física. Alteridad, 17(1), 12–23.* https://doi org/10.17163/ALT.V17N1.2022.01

Moral Muñoz, J. A., Pacheco Serrano, A. I., Lucena Anton, D., & Cobo, M. J. (2019). *Discovering Rehabilitation trends in Spain: A bibliometric analysis. Procedia Computer Science, 162, 770–777.* https://doi.org/10.1016/J PROCS.2019.12.049

Murillo León, M. C., Baquero Valdés, F., & Sotelo Saiz, A. (2017). *Los juegos de guerra en la formación profesional militar. Ciencia y Poder Aéreo, 11(1).* https://doi.org/10.18667/CIENCIAYPODERAEREO.521

Decreto 338 - *Establecer los lineamientos generales para fortalecer la gobernanza de la seguridad digital., Presidencia de la Republica de Colombia 1 (2022).*

Prins, A. A. M. (1990). *Behind the scenes of performance: Performance, practice and management in medical research*. Research Policy, 19(6), 517–534. https://doi.org/10.1016/0048-7333(90)90010-4

Priyadarshini, I., & Barner, K. E. (2018). *Features and architecture of the modern cyber range: a qualitative analysis and survey*. https://udspace.udel edu/handle/19716/23789

Sá Carvalho, M., Travasso, C., y Medina, C. (2014). Redes de cooperación científica. Rio de Janeiro, 30(2), 225-227.

Sancho Núñez, J. C., Pablo Rodríguez, D. M., & Caro Lindo, A. (2021). *Guía de resolución de pruebas CTF para adquirir habilidades de seguridad informática y análisis forense.* https://doi.org/10.18239/Jornadas_2021.34.62

Schwab, K. (2016). The Fourth Industrial Revolution: what it means and how to respond. World Economic Forum.

Singer, P. W., & Friedman, A. (2013). Cybersecurity and Cyberwar: What Everyone Needs to Know: What Everyone Needs to Know. En Oxford University Press.

Torres-Salinas, D., & Jiménez-Contreras, E. (2012). *Hacia las unidades de bibliometría en las universidades: Modelo y funciones. Revista Espanola de Documentacion Cientifica, 35(3).* https://doi.org/10.3989 redc.2012.3.959

Túñez López, M., & de Pablos Coello, J. M. (2013). *el 'índice h' en las estrategias de visibilidad, posicionamiento y medición de impacto de artículos y revistas de investigación* (Vol. 1).

Tuñez, M., y de Pablos, J. (2013). *El 'índice h' en las estrategias de visibilidad, posicionamiento y medición de impacto de artículos y revistas de investigación*. ISBN: 978-84-616-4124-6

Urbizagástegui Alvarado, R. (1999). *La ley de Lotka y la literatura de bibliometría. Investigación Bibliotecológica, ISSN-e 0187-358X, Vol. 13, No. 27, 1999, Págs. 125-141, 13(27), 125–141.* https://dialnet.unirioja.es/servlet articulo?codigo=962863