DYNA
http://dyna.medellin.unal.edu.co/

UNIVERSIDAD NACIONAL DE COLOMBIA

Framework for modeling and simulation of maritime cyberdefense - MARCIM: state of the art and methodology

Diego Edison Cabuya-Padilla & Carlos Alfonso Castaneda-Marroquin

Facultad de Ingeniería, Escuela Naval de Cadetes "Almirante Padilla", Cartagena, Colombia. diego.cabuya@enap.edu.co, carlos.castaneda@enap.edu.co

Received: July 28th, 2023. Received in revised form: December 13th, 2023. Accepted: December 15th, 2023.

Abstract
The article presents the state of the art and methodology of the doctoral research project "Framework for modeling and simulation of maritime cyberdefense - MARCIM". The state of the art defined the background of the research problem, the state of scientific activity, trends and challenges related to MARCIM: cyberdefense, modeling and simulation in cyber security and cyberdefense; and maritime cybersecurity and cyberdefense. The methodology was established with a focus on modeling complex systems, by phases and application actors. The article mainly concludes that maritime cyberdefense at a strategic level behaves like a complex system, with dynamics, processes and elements that cannot be clearly identified, which require modeling and simulation, with a metaheuristic approach, to study the set of actions and interactions between its entities.

Keywords: ciberdefense; cybernetics; cybersecurity; defense; informatics; maritime; simulation models.

Marco de referencia para el modelamiento y simulación de la ciberdefensa marítima - MARCIM: estado del arte y metodología

Resumen
El artículo presenta el estado del arte y metodología del proyecto de investigación doctoral "Marco de referencia para el modelamiento y simulación de la ciberdefensa marítima – MARCIM". El estado del arte definió los antecedentes del problema de investigación, estado de la actividad científica, tendencias y retos de las temáticas del MARCIM: ciberdefensa, modelamiento y simulación en ciberseguridad y ciberdefensa; y ciberseguridad y ciberdefensa marítima. La metodología se planteó con un enfoque en modelamiento de sistemas complejos, por fases y actores de aplicación. El artículo concluye principalmente que la ciberdefensa marítima a nivel estratégico se comporta como un sistema complejo, con dinámicas, procesos y elementos que no se pueden identificar claramente, que requieren del modelamiento y simulación, con un enfoque metaheurístico, para estudiar el conjunto de acciones e interacciones entre sus entidades.

Palabras clave: ciberdefensa; cibernética; ciberseguridad; defensa; informática; marítimo; modelo de simulación.

1. Introducción

El artículo presenta los antecedentes, estado del arte y metodología desarrollada para el proyecto de investigación doctoral "Marco de referencia para el modelamiento y simulación de la ciberdefensa marítima – MARCIM" asociado a la Escuela Naval de Cadetes "Almirante Padilla", el cual aborda cuatro problemáticas [1]: falta de estandarización en la gestión de la ciberdefensa a nivel nacional e internacional; pocas iniciativas de modelamiento y simulación para mejorar la rentabilidad y la eficacia operacional de la ciberdefensa; un incremento de los ciberataques al sector marítimo, que evidencian las debilidades y amenazas del sector marítimo en el ciberespacio; y la necesidad de enfocar los esfuerzos de la ciberdefensa marítima a nivel estratégico.

How to cite: Cabuya-Padilla, D.E. y Castaneda-Marroquin, C.A. Marco de referencia para el modelamiento y simulación de la ciberdefensa marítima - MARCIM: estado del arte y metodología. DYNA, 91(231), pp. 169-179, January - March, 2024.

El proyecto MARCIM cobra importancia para el sector marítimo por la necesidad de protección ante ciberataques que salvaguarden las infraestructuras críticas que lo componen y mantengan su estabilidad; por su contribución al Plan de Desarrollo Naval 2042 de la Armada de Colombia [2]; y por la ausencia de investigaciones relacionadas con la ciberdefensa marítima.

El desarrollo del estado del arte y metodología en el MARCIM, contempló dos etapas, la primera etapa, el estado del arte, consistió en definir el marco teórico y los antecedentes del problema de investigación y posteriormente abordar las temáticas más importantes relacionadas con él para determinar el estado de la actividad científica, tendencias y retos alrededor del MARCIM. Las temáticas identificadas y desarrolladas fueron: ciberdefensa, modelamiento y simulación en ciberseguridad y ciberdefensa, y ciberseguridad y ciberdefensa marítima.

La segunda etapa, metodología de modelamiento de sistemas complejos para el MARCIM, es el resultado de la elaboración de los antecedentes, marco teórico y estado del arte, por medio de estudios bibliométricos y análisis bibliográficos de la primera fase. Los resultados de este proceso investigativo permitieron plantear la metodología para responder a la pregunta problema del proyecto de investigación MARCIM y estar acorde a sus necesidades. La metodología se planteó con un enfoque sistémico, con aproximación en sistemas complejos, en fases y actores de aplicación (experto, modelador, ordenador), definiendo el diagrama de flujo y caracterización por cada paso en la fase respectiva.

Este artículo es el resultado de la primera etapa de investigación del proyecto MARCIM, permitiendo el inicio del desarrollo de los objetivos específicos formulados.

2. Marco teórico

2.1 Descripción del problema

La ciberdefensa entendida como el uso de las "capacidades militares ante amenazas cibernéticas, ataques cibernéticos o ante actos hostiles de naturaleza cibernética que afecten la sociedad, la soberanía nacional, la independencia, la integridad territorial, el orden constitucional o los intereses nacionales" [3, pp.88] es un campo académico con pocos años de madurez, empieza desde el 2003 y la producción científica tiene un índice de vida media de 3.4 años, acompañada por una producción anual baja [4], en comparación con áreas como la ciberseguridad con valores de aproximadamente tres veces más [5].

A pesar de la poca producción científica en ciberdefensa, esta es una prioridad internacional. Miembros de la OTAN, como Estados Unidos, Alemania, Francia, Estonia y España; iniciaron desde 2011 la implementación de medidas de ciberdefensa como parte de su estrategia de ciberseguridad nacional, llegando a niveles de desarrollo suficientes para enfrentar las amenazas y retos que supone el ciberespacio con un enfoque en cooperación internacional público y privado, capacidades avanzadas de ciberdefensa, investigación científica, educación, conciencia situacional cibernética y adopción de marcos conceptuales [6, pp.68–78], [7, pp.7–11], así como la implementación de iniciativas de modelamiento y simulación para mejorar la rentabilidad y eficacia operacional en defensa [8, pp.6–10].

En América Latina, se ha avanzado en la gestión de la ciberseguridad y ciberdefensa con la creación de organismos nacionales de ciberseguridad, implementaciones tecnológicas de cobertura nacional, cooperación interinstitucional para la atención de incidentes cibernéticos, entre otros progresos. Sin embargo, su nivel de preparación no es suficiente y se presentan diversas necesidades como la adopción de marcos y modelos conceptuales de ciberdefensa, definición de objetivos y responsabilidades en las estructuras destinadas a atender los asuntos del ciberespacio, implementación de lineamientos para la gestión de los asuntos del ciberespacio a nivel nacional, cooperación en ciberdefensa, diseño de tecnologías de ciberdefensa, desarrollo de leyes orientadas a regular los sectores público y privado en actividades cibernéticas, etc. [9, pp.178], [10, pp.49–62].

Colombia desde el 2011, a través de tres políticas de desarrollo económico y social (CONPES), viene implementando políticas y estrategias de seguridad y defensa en el ciberespacio con un enfoque en gestión de riesgos. Estas medidas han propiciado el fortalecimiento y la generación de capacidades en el ciberespacio, así como la estructura organizacional para su gestión al interior del Ejecutivo [11, pp.10–27], lo que ubica a Colombia en el puesto número 81 del índice de ciberseguridad global, con debilidades manifiestas en las medidas legales y organizacionales y con fortalezas en las medidas técnicas [12].

Sin embargo, el Departamento Nacional de Planeación [11, pp.10–27] asegura que Colombia tiene moderadas capacidades de ciberdefensa que requieren ser mejoradas a razón de tres aspectos: la debilidad en las capacidades en seguridad digital de los ciudadanos, el desarrollo inadecuado del marco de gobernanza de la seguridad digital y la no adopción de modelos, estándares y marcos de trabajo en seguridad digital con énfasis en nuevas tecnologías.

La situación nacional e internacional expuesta refleja la necesidad para los Estados de fortalecer la ciberdefensa en gestión, capacidades y cooperación, como parte de la proyección estratégica de su ciberseguridad nacional [13], [14], adicionalmente, denota la necesidad de desarrollar marcos y modelos teóricos bajo el enfoque de la anticipación [15, pp.20], utilizando herramientas de modelado y simulación de escenarios, redes, efectos y comportamientos [16, pp.65] que optimicen la toma de decisiones.

Dado el contexto expuesto, la ciberdefensa marítima cobra gran importancia por estar enfocada en un sector que mueve más del 90% de la carga económica, además de su fuerte componente tecnológico y enlace con los demás sectores productivos [17], consolidándose como un sector vital para la economía, que debe ser protegido de las amenazas en el ciberespacio, teniendo en cuenta que los

ciberataques a este sector han aumentado un 900% en los últimos 3 años [18–20]. Los ataques dirigidos tanto a tecnologías de información como de operación son una de las principales preocupaciones del sector ya que pueden provocar pérdida de vidas, pérdida de control sobre los barcos y/o carga o los datos confidenciales [18], [21, pp.132,135–136].

En síntesis, el problema de investigación se sustenta en cuatro aspectos [1]:

- Falta de estandarización en la gestión de la ciberdefensa a nivel nacional e internacional.
- Pocas iniciativas de modelamiento y simulación para mejorar la rentabilidad y la eficacia operacional de la ciberdefensa.
- Incremento de los ciberataques al sector marítimo, que evidencian las debilidades y amenazas del sector marítimo en el ciberespacio.
- Necesidad de enfocar los esfuerzos de la ciberdefensa marítima a nivel estratégico.

2.2 Proyecto de investigación MARCIM

Dado el problema planteado se requiere implementar marcos y modelos para optimizar la toma de decisiones y gestión de recursos de la ciberdefensa marítima a nivel estratégico que garanticen el normal desempeño de las actividades marítimas en el ciberespacio y la resiliencia en el caso de una afectación. Lo anterior, llevó a plantear la siguiente pregunta de investigación [1]: ¿Cuál es el comportamiento de la ciberdefensa marítima a nivel estratégico dentro de un conjunto de acciones e interacciones entre sus entidades?

Para abordar la pregunta de investigación se formuló el proyecto de investigación doctoral "Marco de referencia para el modelamiento y simulación de la ciberdefensa marítima – MARCIM" asociado a la Escuela Naval de Cadetes "Almirante Padilla", que tiene como objetivo general formular un marco de referencia para el modelamiento y simulación de la ciberdefensa marítima a nivel estratégico, y como objetivos específicos:

- Explicar los requerimientos del marco de referencia para el modelamiento y simulación de la ciberdefensa marítima a nivel estratégico.
- Diseñar un modelo de simulación de las acciones e interacciones entre las entidades de la ciberdefensa marítima a nivel estratégico.
- Validar conceptual y operativamente el modelo de ciberdefensa marítima a través de simulaciones.

2.3 Justificación del MARCIM

La ciberdefensa marítima en Colombia es liderada por la Armada Nacional a través de la Dirección Cibernética Naval, contando con unos avances destacados en ciberseguridad, ciberdefensa y ciberinteligencia, aumentando así las capacidades de detección, gestión y análisis de eventos e incidentes en el ciberespacio. Adicionalmente, las estrategias de defensa de la Armada "contemplan el crecimiento y desarrollo tecnológico de capacidades de detección, contención y respuesta a las amenazas cibernéticas que afecten las operaciones militares y la infraestructura crítica cibernética de la nación" [22].

Dichas estrategias de defensa de la Armada, estipuladas en el Plan de Desarrollo Naval 2042, incluyen dentro de sus objetivos de desarrollo tecnológico "generar autonomía, reducir dependencia tecnológica y obtener ventajas operacionales a través de los procesos de I+D+i que fortalezcan el desarrollo tecnológico de la institución" a través del desarrollo de "software y hardware para detectar, contener y responder a las amenazas cibernéticas que afecten las operaciones militares y la infraestructura critica cibernética de la nación" [2, pp.102–103].

Por otra parte, a pesar de la importancia de la ciberdefensa marítima, esta tiene una producción científica muy baja que se ha estado enfocando principalmente en los buques y no en el poder marítimo como sistema [18], desconociendo que las amenazas cibernéticas, los buques, las terminales portuarias y otros sistemas marítimos evolucionan simultáneamente y que los efectos negativos de los ciberataques son evidentes no solo a bordo del buque víctima, sino en un sector mucho más amplio que incluye compañías navieras, puertos, sistemas de interconexión, etc. [21, pp.138].

Teniendo en cuenta lo anterior, el proyecto MARCIM se justifica por lo siguiente [1]:

- La importancia que reviste para el sector marítimo y la protección ante ciberataques que salvaguarde las infraestructuras críticas que lo componen y mantengan la estabilidad del sector.
- Su contribución al Plan de Desarrollo Naval 2042 de la Armada de Colombia [2] en su objetivo de desarrollo tecnológico con el consecuente fortalecimiento del programa Nacional de Ciencia y Tecnología del Sector Defensa elaborado por el Ministerio de Ciencia, Tecnología e Innovación [23].
- La ausencia de investigaciones relacionadas con la ciberdefensa marítima. Las investigaciones existentes tienen un enfoque en los buques y no en el poder marítimo como sistema.

3. Métodos

El artículo se enfoca en el estado del arte y metodología desarrollada para el proyecto de investigación titulado "Marco de referencia para el modelamiento y simulación de la ciberdefensa marítima – MARCIM", como resultado de la investigación preliminar y que permitió la formulación e inicio del proyecto de investigación. En este sentido, se contemplaron dos etapas de desarrollo.

La primera etapa, el estado del arte, consistió en definir los antecedentes del problema de investigación y posteriormente abordar las temáticas más importantes relacionadas con el tema de investigación para determinar el estado de la actividad científica, tendencias y retos alrededor del MARCIM. Las temáticas identificadas y desarrolladas

fueron: ciberdefensa, modelamiento y simulación en ciberseguridad y ciberdefensa, y ciberseguridad y ciberdefensa marítima.

El procedimiento metodológico en esta etapa consistió primero en realizar un estudio bibliométrico por temática, que inicia con la delimitación espacio temporal, definición de las palabras clave y la sentencia de búsqueda utilizando los diferentes operadores booleanos y conectores. Posteriormente, se aplicó la sentencia de búsqueda en el metabuscador científico Scopus ® [24] y los resultados fueron descargados en un archivo de formato "BibTeX". Utilizando el software R [25] y la librería "Bibliometrix" con Biblioshiny [26], con el fin de realizar el respectivo análisis estadístico y de indicadores bibliométricos, teniendo en cuenta las metodologías dispuestas para ello [27–29]. Producto del análisis bibliométrico se identificó la documentación científica relevante para el estudio de la temática, realizando un análisis bibliográfico de cada documento, y posteriormente un análisis global de los resultados para generar las conclusiones respectivas que constituyen el estado del arte para el MARCIM, y determinan la forma de abordar el problema de investigación.

La segunda etapa, metodología de modelamiento de sistemas complejos para el MARCIM, parte de las conclusiones de la primera etapa, en las que se define, entre otros, el tipo de modelamiento y simulación con el que se abordará la formulación del MARCIM. En este sentido, se realizó un análisis bibliográfico y caracterización de las diferentes metodologías para el modelamiento de sistemas complejos y se desarrolló una metodología acorde a las necesidades del MARCIM. La metodología se planteó con un enfoque en fases y actores de aplicación (experto, modelador, ordenador), posteriormente se determinó el diagrama de flujo respectivo y la explicación de cada paso en la fase respectiva.

4. Resultados

4.1 Estado del Arte

4.1.1 Antecedentes

El estudio bibliométrico y análisis de bibliografía del tema [30] dio como resultado que no se han realizado investigaciones que respondan a la pregunta de investigación planteada para el MARCIM. A continuación, se presentan los trabajos de investigación más cercanos al objetivo general y que muestran el contexto del problema con relación a la teoría y su importancia.

La propuesta de modelado y simulación basado en agentes para el entendimiento de la guerra cibernética entre malefactores y agentes de seguridad en internet de Kotenko [31] aborda el modelado y simulación mediante un análisis de procedimientos de ataque y defensa para "Denegación de Servicio Distribuida" (DDoS), teniendo en cuenta los siguientes aspectos: "actores de diferentes equipos compiten para alcanzar intenciones adversarias, actores del mismo equipo cooperan en intenciones conjuntas, ontologías de los ataques DDoS, y los mecanismos de protección contra ellos" [30]. Estos aspectos son abordados desde un enfoque sistémico, "determinando las variantes de estructuras de equipos de los agentes, mecanismos de interacción y coordinación y especificaciones de jerarquía de planes de acción" [30]. Este trabajo establece unas bases para el desarrollo de modelos más flexibles y dinámicos desde el punto de vista teórico de sistemas complejos, permitiendo valorar y optimizar las capacidades de los equipos de ciberseguridad y ciberdefensa, así como entender el impacto de la cooperación entre organizaciones y componentes. Kotenko también desarrolló una propuesta de modelamiento y simulación de múltiples agentes en escenarios de ciberataque y ciberdefensa a la seguridad nacional [32], con un enfoque en los componentes distribuidos de ciberdefensa de forma cooperativa, utilizando simulación basada en agentes y simulación de eventos discretos aplicada a ciberataques y mecanismos de protección cibernética multiagente, llegando hasta el nivel de intercambio de paquetes en protocolos de red. La investigación propone un marco común para implementar entornos de simulación multiagente, realizar experimentación y probar escenarios de ataques a redes distribuidas y mecanismos de defensa; "evidenciando cómo la cooperación en ciberdefensa, la identificación de múltiples escenarios de ataque y defensa cibernética y el cálculo de la probabilidad de éxito conducen a la mejora esencial de la efectividad de la defensa" [30].

Dobson y Carley [33] formulan un marco común para simular la guerra cibernética con un enfoque basado en agentes, el Cyber Forces Interactions Terrain - Cyber FIT (Fuerzas Cibernéticas de Interacción en Terreno), que proporciona los elementos necesarios para facilitar el planeamiento militar de la fuerza cibernética en diferentes terrenos y contra varias fuerzas adversas, mediante una simulación y predicción de los resultados de la guerra cibernética, determinando aspectos como vulnerabilidades, degradación de activos y tasa de capacidad de la misión, por medio del análisis de tres elementos principales: fuerzas, interacciones y terreno. El desarrollo se hizo bajo una visión sistémica y holística de la conducción de la guerra, utilizando el modelado basado en agentes en el software NetLogo [34], obteniendo como resultado un entorno de simulación de la guerra cibernética que necesita perfeccionarse mediante el uso de datos operacionales reales. Se resalta el uso de técnicas de modelamiento de sistemas complejos, como el modelamiento basado en agentes, tratando a cada fuerza de tarea como un agente complejo que toma decisiones inciertas que dependen de los otros elementos, terreno e interacciones; lo que la hace una aproximación de interés para abordar la complejidad de acciones e interacciones entre los agentes del poder marítimo.

El marco de referencia para la evaluación del riesgo cibernético marítimo basado en modelamiento– MACRA de Tam y Jones [35] considera una combinación de amenazas cibernéticas y factores marítimos, enfrentados con una variedad de funcionalidades, configuraciones, usuarios y factores ambientales del ambiente marítimo, con el objetivo de presentar de manera integral los riesgos cibernéticos marítimos y apoyar la toma de decisiones en seguridad cibernética marítima. Considera tres ejes de evaluación de

riesgo: atacante, vulnerabilidad y medidas de mitigación, con sus respectivas variables y atributos, permitiendo el análisis de diferentes combinaciones de efectos de amenazas cibernéticas sobre sistemas y tecnologías a bordo de los buques. Los diferentes escenarios de evaluación de riesgo descritos en el trabajo muestran que, aunque la metodología y función objetivo del modelo tiene un enfoque de ciberseguridad de buque, estos son aplicables al desarrollo del objetivo de la presente investigación, constituyéndose como una de las pocas aproximaciones de modelamiento de amenazas cibernéticas en el escenario marítimo, mostrando una gran flexibilidad de adaptación y aplicabilidad por el uso de datos situacionales.

Finalmente, el estudio de modelamiento y simulación de sistemas complejos para gobernanza de Katina y otros [36] presenta opciones para utilizar el modelamiento y simulación en sistemas complejos relacionados con la gobernanza, evaluando diferentes paradigmas de compatibilidad a través de una revisión extensa de literatura en las que se definen las tendencias actuales de modelamiento y simulación, incluyendo software, para finalmente proponer la necesidad de desarrollar un modelo híbrido basado en tres paradigmas de modelamiento y simulación: agentes, eventos discretos y dinámica de sistemas; ajustados a las necesidades de gobernanza de sistemas complejos actuales y proyectados. Este trabajo es un referente importante porque establece un estado del arte de modelamiento y simulación de estos sistemas, sugiriendo para su abordaje la combinación de técnicas de modelado y simulación. Igualmente, pone a consideración las restricciones de datos e información en sistemas de gobernanza por temas de reserva, situación que puede llegar a limitar la precisión de los modelos y hacerlos poco realistas.

Los antecedentes evidencian que la aproximación al modelamiento y simulación en ciberdefensa marítima debe hacerse desde el enfoque sistémico, principalmente como un sistema complejo por tener varios niveles de organización e interacción y múltiples agentes (actores, entidades, sistemas, etc.) con un grado de autonomía significativo. Adicionalmente, debe incluir la identificación y estudio de escenarios de ataque y defensa, junto con sus respectivos cálculos de riesgo y probabilidad de éxito, que permitan a los experimentadores probar cuantitativamente hipótesis de trabajo o cursos de acción.

4.1.2 Ciberdefensa

En la temática ciberdefensa, la bibliometría [4] presenta un total de 641 documentos afines al tema, elaborados en el lapso entre 1992 y 2020 con un porcentaje de crecimiento anual del 22.16%, mostrando el auge y actual interés en el tema. El país con mayor producción en el tema es Estados Unidos, con una producción de 325 artículos, seguido por Reino Unido (38), India (21) y China (19). Los autores más productivos son Liu P., Pal P., Jacobson D., Rursch J.A., Mehtre B. M.; los más citados son Liu P., Hwang K., Ku W. -S. y Chen Y., quienes representan el 50 % de las citaciones en el campo de la ciberdefensa, el 34,5 % de los autores no cuentan con ninguna citación. Las tendencias de investigación están centradas en la gestión de la ciberseguridad, cibercrimen y ciberataques [4].

Del análisis bibliográfico de los documentos encontrados se resaltan seis de ellos, adicionales a los trabajos de Kotenko [31,32] abordado en los antecedentes. El artículo Teoría de juegos para ciberseguridad [37], resalta que las soluciones de ciberseguridad escasean principalmente en los casos de marcos de decisión cuantitativo, por lo cual no responden a los cambios dinámicos de los escenarios de ataque. Los autores utilizan la teoría de juegos para crear un marco analítico sólido para analizar la interacción entre los ataques y los mecanismos de ciberdefensa y proponen una arquitectura de ciberdefensa inspirada en esta teoría. La aproximación metodológica es holística, siguiendo las bases de un juego estocástico de información imperfecta.

El marco basado en agentes para el conocimiento de la situación cibernética de Bradshaw y otros [38], busca aumentar la percepción y la cognición humana alrededor de la ciberseguridad y ciberdefensa, y optimizar cualitativamente en la conciencia situacional cibernética. El enfoque metodológico usa un marco basado en agentes que explora la comprensión de situaciones complejas a través de la colaboración y el entendimiento de la ciberseguridad y ciberdefensa, lo que los autores denominan 'construcción de sentido distribuida'. Un aporte importante de este trabajo es la incorporación del factor humano como eje central del marco de ciberseguridad y ciberdefensa propuesto, y su tratamiento como un agente imperfecto y de comportamiento aleatorio.

El marco para la asignación y ubicación óptima de sistemas de ciberdefensa en redes de detección de intrusiones – DEFIDNET de Pastrana y otros [39], presenta un modelo de distribución de contramedidas cibernéticas basadas en algoritmos de optimización multiobjetivo, con el propósito de implementar estrategias de asignación que optimicen la gestión del riesgo [18], [39]. El esquema propuesto se centra en un análisis nodal de la probabilidad de propagación de un ciberataque en toda la red y las posibles rutas de afectación, generando la información suficiente para optimizar los sistemas de ciberdefensa.

El marco para mejorar los juegos de guerra cibernéticos (*Cyber Wargaming*) en un contexto empresarial realista de Bodeau [40] y el marco conceptual para el desarrollo de juegos serios de ciberseguridad propuesto por Katsantonis [41], tienen en común el uso de juegos serios y enfoques de aprendizaje basados en juegos para generar conocimiento en ciberseguridad y ciberdefensa, ambos se presentan de forma general, pero muestran facilidades de adaptación para garantizar que los ejercicios de juegos de guerra reflejen con precisión la eficacia del entorno tecnológico y de gestión de riesgos. Para el caso de Bodeau y otros [40], el marco se describe en términos de protección de sistemas en el sector de servicios financieros (FSS), pero que tiene aplicación en otras infraestructuras críticas, equilibrando el fuerte enfoque de la tecnología de ciberdefensa de los ejercicios de formación de equipos cibernéticos, con el enfoque sólido del impacto comercial y operativo, típico de los ejercicios de mesa de alto nivel centrados en el ciberespacio. El documento resalta que los marcos existentes de juegos de

guerra son suficientes para apalancar modelos de escenarios compuestos de juegos de guerra cibernéticos para que una institución pueda producir un realismo mejorado, reducir el impacto y el riesgo de los adversarios cibernéticos. Sin embargo, requiere un componente tecnológico avanzado que mejore la simulación, orquestación y medición de los resultados de los ejercicios. El marco de Katsantonis y otros [41], se encuadra en la educación y concientización en ciberseguridad y ciberdefensa, promoviendo enfoques basados en juegos que prevean la mejora de la eficacia pedagógica de la educación en ciberseguridad y ciberdefensa mediante la adopción de teorías de aprendizaje modernas y enfoques de enseñanza innovadores, en el marco de un ciclo de vida de aprendizaje sostenible.

La Guía de Ciberdefensa: orientaciones para el diseño, planeamiento, implantación y desarrollo de una ciberdefensa militar, elaborada por la Junta Interamericana de Defensa [16] proporciona un modelo operativo de la ciberdefensa a nivel estratégico, desde una perspectiva operativa militar que facilite la interacción con los diferentes dominios de la guerra. Aunque el documento se enmarca en el mundo organizacional, es un referente para entender la ciberdefensa desde el punto de vista de seguridad nacional y de cooperación internacional, que evidencia la necesidad de establecer marcos de referencia en la gestión de la ciberdefensa y la aplicación de modelamiento y simulación para optimizar la toma decisiones en el dominio del ciberespacio, el quinto dominio de la guerra.

4.1.3 Modelamiento y simulación en ciberseguridad y ciberdefensa

En la temática de modelamiento y simulación en ciberseguridad y ciberdefensa la bibliometría [30] se encontraron 994 documentos del tema, entre los años 2002 y 2021 con un porcentaje de crecimiento anual del 23.26%, que refleja la importancia actual del tema para el ambiente académico. El país con mayor producción es “Estados Unidos con 155 artículos, seguido de China (36) y otros países como India (27), Reino Unido (21) y Australia (17). Los autores más productivos son Lakhno V., Mylrea M., Gourisetti SNG., Li S. y Pietre-Cambacedes L.” [30]; el mayor nivel de dominancia lo tienen Gourisetti SNG., Quinn EL. y Lakhno V.; el mayor índice h son los de Mylrea y Ekstedt; el índice g más alto es el de Chen y Ekstedt; y el mejor índice m son los de Lakhno y Gourisetti. El país con más cooperación y coautorías es Estados Unidos, cooperando con siete países principalmente: Reino Unido, Corea, China y Arabia Saudita; “así mismo, India está unido con seis países, destacando conexiones con Canadá, España, Australia y China; y por su parte Italia se relaciona también con seis países, destacando las conexiones con Estados Unidos, Australia, Suecia y Polonia [30].

A través de un ACM (Análisis de Correspondencias Múltiples) de las coocurrencias del tema se determinaron cuatro áreas de investigación: la primera, la transmisión de energía eléctrica y microrredes; la segunda, los sistemas de control industrial e infraestructuras críticas cibernéticas industriales; la tercera, la gestión de riesgos cibernéticos, gestión de la información y controles de seguridad de la información; y la cuarta, la ciencia de datos, modelamiento y simulación [30].

Del análisis bibliográfico de los documentos encontrados se resaltan seis de ellos, adicionales a los trabajos de Dobson y Carley [33] y Katina y otros [36] abordados en los antecedentes. El estudio de la ciberdefensa como un sistema adaptativo complejo [42] resalta que las tecnologías cibernéticas empresariales a menudo se implementan sin tener en cuenta las interacciones que ocurren entre los humanos y la nueva tecnología. Además, las interacciones que ocurren entre individuos a menudo también pueden tener un impacto en la tecnología recientemente empleada. Teniendo en cuenta lo anterior, el documento presenta el estudio de un escenario en el que una agencia gubernamental hipotética aplica una perspectiva de la ciencia de la complejidad, respaldada por modelos basados en agentes, para comprender mejor los impactos de las decisiones de política estratégica, que lleva a la construcción de un modelo para explorar la dinámica sociotécnica de estos sistemas.

El modelo de ciberataques y ciberdefensas en sistemas de medición local [43], el modelo dinámico de mitigación de ataques para el análisis de vulnerabilidades de seguridad en un sistema de energía ciber-físico [44], y el modelo para la defensa de los sistemas de energía contra ciberataques dinámicos con enfoque en teoría del juegos [45], tienen en común que abordan la ciberseguridad y ciberdefensa en sistemas de energía buscando la mitigación del riesgo a ciberataques, mediante la metodología de teoría de juegos dinámicos con información incompleta, modelando las interacciones entre un atacante y un defensor, para facilitar los procesos de asignación y distribución de recursos de ciberdefensa en los sistemas de energía; mejorar la resiliencia de los sistemas ante ataques dinámicos; evaluar las vulnerabilidades; y generar estrategias de protección efectivas contra diferentes combinaciones de ataques.

El modelo *Hybrid Cyber Kill Chain* (Cadena de Muerte Cibernética Híbrida) [46], presenta el estudio de diferentes modelos aceptados de ciberataques y proponen una nueva aproximación de modelamiento de la *Cyber Kill Chain* (Cadena de Muerte Cibernética) bajo un concepto híbrido, considerando las fortalezas de los actores de amenazas y defensores, utilizando la metodología de redes de petri de colores para el análisis. El marco de referencia y modelo resultante permite ayudar a las organizaciones empresariales a tomar medidas para hacer frente a los incidentes cibernéticos, minimizando o eliminando el impacto, y estableciendo los controles y contramedidas necesarias.

El modelo de apoyo a la toma de decisiones para la estimación de efectos y evaluación de proporcionalidad en operaciones cibernéticas [47], permite el cálculo y clasificación de los efectos de las operaciones cibernéticas, y la evaluación de la proporcionalidad para apoyar las decisiones en las operaciones cibernéticas mediante el diseño e implementación de un modelo difuso de varias capas, que incluye el análisis de operaciones cibernéticas reales y virtuales, combinadas con entrevistas y grupos focales con expertos técnicos y militares.

Esta investigación deja en evidencia la necesidad de metodologías y modelos para planificar, ejecutar y evaluar la ciberdefensa de forma responsable, y presenta una metodología aplicable a otros escenarios.

4.1.4 Ciberseguridad y ciberdefensa marítima

Finalmente, en la temática de ciberseguridad y ciberdefensa marítima la bibliometría [18] encontró 153 del tema, entre 1999 y 2021 con un porcentaje de crecimiento anual del 3.2%, indicando un limitado interés y desarrollo científico a pesar de que la investigación va en aumento. China es el país con mayor producción, 13 artículos, seguido de Reino Unido (9), Estados Unidos (7) y Noruega (5). Kavallieratos G., Silverajan B., Svilicic B., Brosset D. y Deng R son los autores con mayor producción científica; Kavallieratos, Svilicic y Kamahara el índice h más alto;Svilicic B., Tam K. y Yang T. tienen el mayor nivel de dominancia; Kavallieratos y Svilicic el índice g más alto y; Svilicic y Kamahara el índice m más alto. Reino Unido y Noruega son los países con más cooperación de coautorías, trabajando con países como Grecia y Alemania; adicionalmente, se resalta la cooperación entre China y Canadá, Estados Unidos con Nueva Zelanda y, Japón con Croacia y Suecia [18].

Analizando las coocurrencias de palabras mediante un ACM (Análisis de Correspondencias Múltiples) se determinaron cuatro áreas de investigación: la primera, criptografía y sistemas de seguridad de la información; la segunda, sistemas de control industrial y sistemas ciberfísicos; la tercera, gestión de riesgos cibernéticos, seguridad marítima y crimen cibernético; y la cuarta, sistemas de control marítimo, ciencia de datos, actividades marítimas, y conciencia cibernética [18].

Del análisis bibliográfico de los documentos encontrados se resaltan tres trabajos, adicionales al trabajo de Tam &Jones [35] abordado en los antecedentes. El estudio de la detección de ciberataques en tiempo real como herramienta para generar una conciencia situacional de los riesgos cibernéticos en los sistemas navales de Jacq y otros [48], que resalta el aumento de los sistemas tecnológicos a bordo de los buques entendiéndolos como un sistema complejo de información en movimiento, con todas las funciones de un sistema convencional. Por lo anterior, la generación de conciencia situacional de los riesgos cibernéticos en los sistemas navales se vuelve una tarea fundamental para el sector marítimo, y la investigación presenta como curso de acción el estudio de ataques en tiempo real, que incluye la recopilación y fusión datos provenientes de los buques, visualización de datos y el intercambio de situaciones entre los actores marítimos.

El estudio de la gestión del riesgo cibernético marítimo desde el punto de vista de Tam y Jones [35], evidencia la necesidad de estudiar la ciberseguridad marítima con un enfoque holístico, por el incremento de la complejidad, la digitalización y la automatización de los sistemas en la industria marítima, así como por el gran número de sistemas interconectados entre el barco y la tierra. Dada esta complejidad, la preocupación del entorno marítimo se está volcando a reducir la vulnerabilidad a los ciberataques y por consiguiente los incidentes cibernéticos, ya que estos en el entorno marítimo "pueden provocar pérdida de vidas, pérdida de control sobre los barcos o los datos confidenciales, así como el secuestro de barcos y/o carga" [18,21, pp.132, 135–136].

El marco de referencia para la ciberinteligencia de amenazas a la infraestructura marítima desarrollado por Pitropakis y otros [49] propone un marco de inteligencia de amenazas para las infraestructuras marítimas que se adapte a la recopilación y análisis de inteligencia de amenazas en estos entornos, combinando la recopilación de datos de sensores de barcos, datos disponibles públicamente de las redes sociales, variedad de *honeypots* (señuelos cibernéticos) que emulan diferentes componentes de hardware y software, detección de eventos asistida por aprendizaje profundo, implementación de *blockchain* (cadenas de bloques) para mantener un registro de auditoría de actividades y transacciones, identificaciones electrónicas y análisis visual de amenazas. La investigación tiene un enfoque centrado en las necesidades marítimas, mostrando sistemáticamente las relaciones entre diferentes actores y las interacciones que se pueden dar entre estos, pero dejando abiertas las posibilidades a investigaciones que orquesten sistemáticamente los diversos escenarios que se dan en el ejercicio de la ciberdefensa.

4.2 Metodología de modelamiento de sistemas complejos para el MARCIM

Para abordar el proyecto de investigación del MARCIM, se desarrolló una propuesta de procedimiento metodológico orientado al modelamiento de sistemas complejos, enfoque sistémico, teniendo en cuenta los resultados del marco teórico, antecedentes y estado del arte. Para ello se establecen tres fases como se muestra en la Fig. 1.

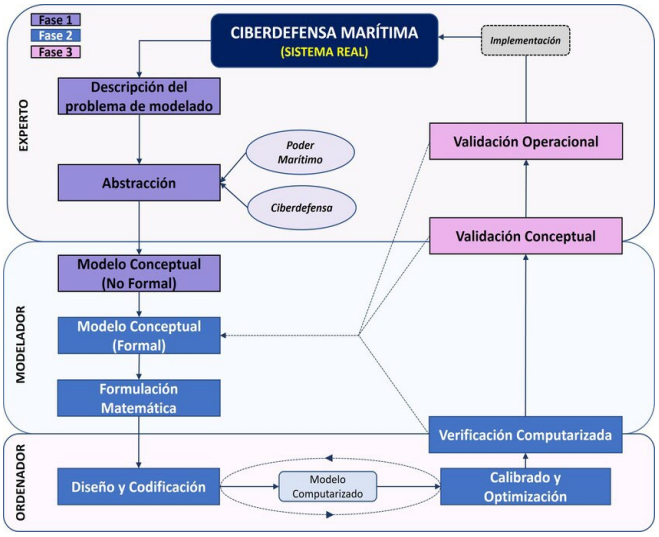

Figura 1: Proceso metodológico MARCIM.
Fuente: Elaboración propia adaptado de [50–52,53, p.186].

4.2.1 Fase 1 – Requerimientos del modelo

La primera fase busca explicar los requerimientos del marco de referencia para el modelamiento y simulación de la ciberdefensa marítima a nivel estratégico, siguiendo los procedimientos relacionados a continuación:

Descripción del problema de modelado: define la perspectiva del modelo así como los aspectos más relevantes del sistema real con el propósito de definir los objetivos que se pretenden alcanzar [50, p. 14], [51, pp. 93–95], describiendo aspectos como: objetivos de modelado, hipótesis de modelado (asunciones), restricciones, tipos de datos y tipos de resultados.

Abstracción: identificación de los componentes más importantes de los sistemas reales, taxonomías, interacciones que pueda existir entre ellos y relaciones causales más significativas, dando como resultado un grupo de modelos no formales que en su conjunto representan el objetivo de modelado [51, pp.93–97], que para esta investigación se concentran en dos sistemas principales: sistema del poder marítimo y sistema de la ciberdefensa.

Modelo conceptual del sistema de ciberdefensa marítima (Modelo no formal): modelo no formal que representa el objetivo de modelado en su contexto general, integrando los sistemas caracterizados en la abstracción. Este procedimiento incluye el desarrollo de taxonomías que apoyen el entendimiento del sistema y estandaricen los elementos de mando y control esenciales para la toma de decisiones y definición de cursos de acción en ciberdefensa marítima, de manera que se puedan generar respuestas colaborativas y coordinadas en todo el sistema, cuando una situación ponga en riesgo algún activo o infraestructura crítica cibernética marítima [54].

4.2.2 Fase 2 - Modelado

La segunda fase aborda el diseño del modelo de simulación de las acciones e interacciones entre las entidades de la ciberdefensa marítima a nivel estratégico, partiendo del modelo conceptual no formal de la primera fase, y se seguirán los siguientes procedimientos:

Modelo conceptual del sistema de ciberdefensa marítima (Modelo formal): caracterización detallada del modelo conceptual que incluye [50, pp. 15–28]: caracterización de variables y componentes del sistema, caracterización de acciones e interacciones, descripción de las relaciones causales (causa-efecto) y descripción de las relaciones funcionales.

El modelo conceptual permite al experimentador, investigador o tomador de decisiones entender "la dinámica del fenómeno estudiado en los correspondiente a actores, acciones e interacciones, y se enmarca como una herramienta de trabajo para la toma de decisiones a nivel estratégico, con miras al cumplimiento de los objetivos de ese nivel" [55].

Formulación matemática del modelo: revisión del modelo formal y concretar la representación del modelo bajo un marco matemático [56].

Diseño y codificación: diseño e implementación del modelo o conjunto de modelos formales en un soporte dinámico, a través de un modelo para computadora, que satisfaga las especificaciones y representaciones planteadas, utilizando herramientas computacionales para modelamiento y simulación, e incluye los siguientes pasos [50, pp.28–29], [51, pp.93–97]: análisis y gestión de la información del modelo (inferencia), selección de las técnicas de modelado para la implementación del modelo conceptual en las herramientas computacionales, selección de las herramientas computacionales e implementación computacional del modelo.

Calibrado y optimización del modelo: permite corregir los parámetros del modelo no determinados y ajustar los parámetros desconocidos [50, pp.33–34].

Verificación computarizada del modelo: comprueba que la implementación del modelo conceptual da los resultados esperados cuando trabaja con escenarios conocidos, mediante el análisis e interpretación del modelo [50, pp.33–34], [51, pp. 97], [53, pp.188–189].

Para la formulación matemática se utilizarán los métodos de simulación y modelado descritos por Alfonso Urquía y Carla Marín (2016), principalmente los estocásticos para simulación probabilística; métodos matemáticos para modelos basados en agentes [56]; y lo descrito en el libro *Simulation Modeling and Analysis* (Modelos de simulación y análisis) [57], principalmente en los métodos de modelamiento de sistemas complejos, modelamiento basado en agentes y sistemas dinámicos. Finalmente, para el diseño, calibrado y verificación computarizada del modelo se contempla el software NetLogo [34], un entorno de modelado programable de múltiples agentes desarrollado por el Center for Connected Learning and Computer-Based Modeling (Centro de aprendizaje conectado y modelado basado en computadora) de la Universidad de Northwestern, caracterizado por su alta escalabilidad, gran fuerza de modelado computacional y baja complejidad de esfuerzo de desarrollo en comparación con otras soluciones [58].

La aplicación de Netlogo será complementada con desarrollos en el área de análisis de datos y algoritmos de aprendizaje (*Machine Learning*) con el software Python [59].

4.2.3 Fase 3 – Validación del modelo

Por último, la tercera fase busca validar el modelo de ciberdefensa marítima a través de simulaciones, para ello se establecen dos tipos de validación:

Validación conceptual (juicio de expertos): determina que las teorías y los supuestos subyacentes al modelo conceptual son correctos y la representación de la entidad problemática, estructura, lógica y relaciones causales del modelo son acordes para el objetivo previsto [53, pp.188].

Validación operacional (juegos de guerra - simulación militar): establece "si el comportamiento de salida del modelo de simulación tiene la precisión requerida para el propósito previsto del modelo sobre el dominio de la aplicabilidad prevista" [53, pp.189]. Para ello se utilizarán los juegos de guerra como herramienta metodológica [60] que

permite explorar las posibilidades de toma de decisiones en un entorno con información incompleta e imperfecta [61], en un escenario hipotético del poder marítimo colombiano.

5. Discusión

5.1 Estado del Arte

5.1.1 Ciberdefensa

Es importante tener presente que la ciberdefensa viene considerando la teoría de juegos y el uso de juegos serios como herramientas metodológicas para optimizar la gestión de sus actividades, así como reducir el impacto y el riesgo de los ciberataques. Igualmente, se evidencia la presencia de escenarios de ataque y defensa dinámicos, que demandan soluciones que evalúen las situaciones desde un enfoque holístico, adaptándose a la complejidad y que incluyan aspectos como el factor humano y la información imperfecta.

5.1.2 Modelamiento y simulación en ciberseguridad y ciberdefensa

La ciberdefensa involucra la interacción entre los humanos y la nueva tecnología, por lo que toma una connotación de sistema complejo que requiere de la implementación de metodologías y modelos para su planificación, ejecución y evaluación, así como el modelamiento de las interacciones entre atacantes y defensores para hacer frente a los incidentes cibernéticos, minimizando o eliminando el impacto, y estableciendo los controles y contramedidas necesarias. Entre las metodologías más usadas en los estudios está el modelamiento basado en agentes, dinámica de sistemas y la teoría de juegos dinámicos con información incompleta.

5.1.3 Ciberseguridad y ciberdefensa marítima

Los estudios de ciberseguridad y ciberdefensa marítima se vienen enfocando principalmente en el buque y son pocos los estudios que abordan la problemática desde un enfoque holístico, es decir, del sistema marítimo en su complejidad, a pesar de que ya se ha evidenciado esta necesidad.

A nivel general, las tres temáticas analizadas (ciberdefensa, modelamiento y simulación en ciberseguridad y ciberdefensa, y ciberseguridad y ciberdefensa marítima) muestran una baja producción científica, con vacíos en la literatura, principalmente en el área de ciberseguridad y ciberdefensa marítima, con diversas oportunidades de investigación, centradas principalmente en los enfoques holísticos de la ciberseguridad y ciberdefensa, así como el uso de metodologías de modelamiento y simulación. Adicionalmente, el análisis bibliográfico establece que para el desarrollo del objetivo de investigación es importante tener presente la multiplicidad y complejidad de las dinámicas de los actores de la ciberdefensa, por lo que se contempla el uso de aspectos relacionados con el enfoque de sistema, específicamente sistemas complejos, abordando el modelamiento y simulación con métodos de ciencia de datos, modelamiento basado en agentes y dinámica de sistemas.

Así pues, el proyecto de investigación MARCIM pretende aportar al estudio de la ciberdefensa marítima desde el modelamiento y simulación con el propósito de establecer un marco de referencia que permita comprender la complejidad de la ciberdefensa marítima y sus procesos fundamentales.

5.2 Metodología de modelamiento de sistemas complejos para el MARCIM

La metodología desarrollada se plantea con un enfoque de sistema (pensamiento sistémico), específicamente sistemas complejos, buscando ofrecer un entorno de simulación en ciberdefensa marítima a nivel estratégico que permita a experimentadores comprender la complejidad del sistema y sus procesos fundamentales, así como estudiar dinámicas, procesos, acciones e interacciones, y elementos que no se pueden identificar claramente, que requieren del modelamiento y simulación.

Adicionalmente, esta metodología puede ser adaptada a entornos de ciberseguridad y ciberdefensa, diferentes al marítimo, en los que existan agentes conectados, interdependientes, diversos, adaptativos y complejos, que requieren de la experimentación con un enfoque metaheurístico para ser estudiados. Entendiendo la metaheurística como la exploración con espacios, conjuntos o redes de soluciones, donde el investigador busca que el sistema se comporte como él desearía [62, pp. 10].

6. Conclusiones

La elaboración de los antecedentes, marco teórico y estado del arte, por medio de estudios bibliométricos y análisis bibliográfico, permitieron plantear la metodología que para responder la pregunta problema del proyecto de investigación MARCIM. Esta metodología tiene un enfoque sistémico, sistemas complejos, y aborda principalmente el ejercicio de la ciberdefensa en el contexto de la ciberseguridad marítima.

La ciberdefensa tiene un comportamiento complejo que involucra la interacción entre los humanos y la nueva tecnología, requiriendo herramientas metodológicas para planificar, ejecutar, evaluar y optimizar la gestión de sus actividades, así como reducir el impacto y el riesgo de los ciberataques. En este sentido, la ciberdefensa se apoya de herramientas como: la teoría de juegos y el uso de juegos serios; teoría de sistemas complejos; modelamiento y simulación de las interacciones entre atacantes y defensores para hacer frente a los incidentes cibernéticos; modelamiento basado en agentes, dinámica de sistemas y la teoría de juegos dinámicos con información incompleta.

Son pocos los estudios relacionados con ciberseguridad y ciberdefensa marítima, y los que existen se enfocan principalmente en el buque, siendo pocos los estudios con un enfoque holístico. Enfoque necesario por la multiplicidad de

actores y dinámicas complejas en el sector marítimo, que requieren su estudio como sistema.

La ciberdefensa marítima a nivel estratégico se comporta como un sistema complejo, con dinámicas, procesos y elementos que no se pueden identificar claramente, que requieren del modelamiento y simulación, con un enfoque metaheurístico, para estudiar el conjunto de acciones e interacciones entre sus entidades.

El proyecto de investigación MARCIM pretende aportar al estudio de la ciberdefensa marítima desde el modelamiento y simulación con el propósito de establecer un marco de referencia que ofrezca un entorno de simulación en esta área que permita a experimentadores comprender la complejidad del sistema y sus procesos fundamentales; desarrollar y probar hipótesis de trabajo o cursos de acción; lograr ver emergencias, dinámicas, procesos, elementos clave a nivel estratégico; prever el comportamiento de las entidades en la ciberdefensa marítima y determinar posibles escenarios de ataque y defensa cibernética en el ámbito marítimo.

Referencias

[1] Cabuya-Padilla, D.E., Framework for modeling and simulation of maritime cyberdefense at strategic level – MARCIM. Doctoral Thesis. Escuela Naval de Cadetes "Almirante Padilla", Cartagena, Colombia, 2021.

[2] Armada República de Colombia. Plan de Desarrollo Naval 2042. Jefatura de Planeación Naval, Dirección de Planeación Estratégica, editors. ARC; [en línea]. Bogotá, Colombia, 2020, 135 P. Disponible en: https://www.escuelanaval.edu.co/es/file-download/download/public/14011

[3] Departamento Nacional de Planeación. Documento CONPES 3854 - Política Nacional de Seguridad Digital. Consejo Nacional de Política Económica y Social. [en línea]. BogotáColombia, 2017. Disponible en: https://colaboracion.dnp.gov.co/CDT/Conpes/Económicos/3854.pdf

[4] Valencia-Arias, A., Patiño-Toro, O., Arenas-Fernández, A., Garcés-Giraldo, L.F., Umba-López, A.M. y Benjumea-Arias, M.L., Tendencias investigativas en el estudio de la ciberdefensa: un análisis bibliométrico. RISTI - Rev Iber Sist e Tecnol Inf - RISTI. [en línea]. (E29), pp. 366–379, 2020. Disponible en: http://www.risti.xyz/issues/ristie29.pdf

[5] Shukla, G., and Gochhait, S., Cyber security trend analysis using Web of Science: a bibliometric analysis. Eur J Mol Clin Med. 7(6), pp. 2567–76, 2020.

[6] Sabillon, R., Cavaller, V., and Cano, J., National cyber security strategies: global trends in Cyberspace. Int J Comput Sci Softw Eng [en línea]. 5(5), pp. 67–81, 2016. [cited: 2020, Aug 17th]. Available at: www.IJCSSE.org

[7] Baezner, M., and Cordey, S., National Cybersecurity strategies in comparison-challenges for Switzerland Center for Security Studies (CSS). ETH Zürich, [online]. 2019, 33 P., Available at: www.css.ethz.ch

[8] North Atlantic Council. NATO Modelling and Simulation Master Plan. Rome, Italy, 2012, pp. 1-10.

[9] Izaguirre-Olmedo, J., Vista de análisis de los ciberataques realizados en América Latina. INNOVA Research Journal, 3(9), pp. 172–181, 2018. DOI: https://doi.org/10.33890/innova.v3.n9.2018.837

[10] Cornaglia, S. y Vercelli, A.H., La ciberdefensa y su regulación legal en Argentina (2006-2015). URVIO - Rev Latinoam Estud Segur. (20), pp. 46-62, 2017. DOI: https://doi.org/10.17141/urvio.20.2017.2601

[11] Departamento Nacional de Planeación. Documento CONPES 3995 - Política Nacional de Confianza y Seguridad Digital, [en línea]. Consejo Nacional de Política Económica y Social, Bogotá, Colombia, 2020. [cited: 2020, Aug 11th]. Disponible en: https://colaboracion.dnp.gov.co/CDT/Conpes/Económicos/3995.pdf

[12] International Telecommunication Union. Global cybersecurity index. Measuring the digital transformation. [online]. 2020. Available at: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-S.pdf

[13] Organización de los Estados Americanos. Hacia una estrategia nacional de ciberseguridad. México D.F., 2017.

[14] Espinosa, E.I., Hacia una estrategia nacional de ciberseguridad en México. Rev Adm Pública [online]. L(1), pp. 115–146, 2015. [cited: 2020, Aug 18th], Available at: https://revistas-colaboracion.juridicas.unam.mx/index.php/rev-administracion-publica/article/view/19862/17821

[15] Junta Interamericana de Defensa. Informe II Conferencia de Ciberdefensa, [en línea]. Washington, USA, 2020. [cited: 2021, Apr. 14th]. Disponible en: https://www.iadfoundation.org/wp-content/uploads/2020/08/Ciberdefensa10.pdf

[16] Ganuza, N., Guía de ciberdefensa: orientaciones para el diseño, planeamiento, implantación y desarrollo de una ciberdefensa militar. Washington, USA, 2020.

[17] Conferencia de las Naciones Unidas sobre Comercio y Desarrollo - UNCTAD. Review of Maritime Transport 2020. United Nations Conference on Trade and Development. [online]. New York, USA. 2020. Available at: https://unctad.org/system/files/official-document/rmt2020_en.pdf

[18] Alcaide, J.I., and Llave, R.G., Critical infrastructures cybersecurity and the maritime sector. Transportation Research Procedia, 45, pp. 547-554, 2020. DOI: https://doi.org/10.1016/j.trpro.2020.03.058

[19] Hellenic Shipping News Worlwide. Maritime cyber attacks increase by 900% in three years. In: International Shipping News, Piracy and Security News [online]. 2020. [cited: 2021, May 26th]. Available at: https://www.marineinsight.com/shipping-news/maritime-cyber-attacks-increase-by-900-in-three-years/#

[20] Cabuya-Padilla, D.E., Alvarado-Carvajal, C.F., Carrascal-Ortiz, R.A., Riola-Rodríguez, J.M., Fajardo-Toro, C.H. y Escandon-Bernal, S.P., Ciberseguridad y ciberdefensa marítima: análisis bibliométrico años 1990 – 2021. RISTI - Rev Iber Sist e Tecnol Inf., 49, pp. 197-210, 2022.

[21] Mraković, I., and Vojinović, R.. Maritime cyber security analysis – How to reduce threats? Trans Marit Sci., 8(1), pp. 132–139, 2019.

[22] Armada República de Colombia. Portafolio de I+D+i de la Armada de Colombia [en línea]. Bogotá, 2021. Disponible en: https://minciencias.gov.co/sites/default/files/upload/convocatoria/anexo_4._alcance_tematicas_de_las_propuestas.pdf

[23] MinCiencias. Programa Nacional en Seguridad y Defensa. Minciencias. [en línea]. 2013 [cited: 2022, Feb 13th]. Disponible en: https://minciencias.gov.co/node/1130

[24] Elsevier. Scopus [online]. 2023 [cited: 2023, Jan 4th]. Available at: https://www.scopus.com/home.uri?zone=header&origin=

[25] CRAN Project. The Comprehensive R Archive Network [online]. 2020. [cited: 2021, Aug 6th]. Available at: https://cran.r-project.org/

[26] K-Synth Srl. Bibliometrix [online]. 2023. [cited: 2023, Jan 4th]. Available at: https://www.bibliometrix.org/home/

[27] Llerena-Paz, M.A. y Arévalo-Avecillas, M.E., Indicadores bibliométricos: origen, definición y aplicaciones científicas en el ecuadorR. Espí-ritu Emprend TES, [en línea]. 5(1), pp. 130–53, 2021. [cited: 2021, Mar 7]. Disponible en: https://www.scimagojr.com/

[28] Donthu, N., Kumar, S., Mukherjee, D., Pandey, N., and Lim, W.M., How to conduct a bibliometric analysis: an overview and guidelines. J Bus Res. [en línea]. 133(March), pp. 285–296, 2021. Disponible en: https://doi.org/10.1016/j.jbusres.2021.04.070

[29] Ávila-Toscano, J.H., Cienciometría y bibliometría. El estudio de la producción científica. Métodos, enfoques y aplicaciones en el estudio de las Ciencias Sociales, 2018, 316 P.

[30] Villalobos-Álvarez, J.M., Análisis bibliométrico años 2000-2021: modelamiento y simulación en ciberseguridad y ciberdefensa. Rev Derrotero. 15(Seguridad y Defenssa), pp. 77–102, 2021.

[31] Kotenko, I., Agent-Based modeling and simulation of cyber-warfare between malefactors and security agents in Internet. In: Simulation in Wider Europe - 19th European Conference on Modelling and Simulation, ECMS 2005. St. Petersburg, 2005, pp.33-43.

[32] Kotenko, I., Multi-agent modelling and simulation of cyber-attacks and cyber-defense for homeland security. In: 2007 4th IEEE Workshop on Intelligent Data Acquisition and Advanced Computing

Systems: Technology and Applications, IDAACS. St. Petersburg, 2007.
[33] Dobson, G.B., and Carley, K.M., Cyber-FIT: an agent-based modelling approach to simulating cyber warfare. In: Lee, D., Lin, YR., Osgood, N., and Thomson, R., Eds., Social, Cultural, and Behavioral Modeling. SBP-BRiMS 2017. Lecture Notes in Computer Science, vol 10354. Springer, Cham. 2017. DOI: https://doi.org/10.1007/978-3-319-60240-0_18
[34] Wilensky, U., NetLogo, [online]. 2016. [cited: 2021, Jul 13th]. Available at: https://ccl.northwestern.edu/netlogo/
[35] Tam, K., and Jones, K., MaCRA: a model-based framework for maritime cyber-risk assessment. WMU J Marit Aff [online]. 18(1), pp. 129–63, 2019. [cited: 2020, Oct 14th]. Available at: https://doi.org/10.1007/s13437-019-00162-2
[36] Katina, P.F., Tolk, A., Keating, C.B., and Joiner, K.F., Modelling and Simulation in complex system governance. Int J Syst Syst Eng. 10(3), pp. 262–92, 2020.
[37] Shiva, S., Roy, S., and Dasgupta, D., Game theory for cyber security. In: CSIIRW '10: Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research. [online]. Oak Ridge, TN. 2010, pp. 1–4. [cited 2020 Aug 1]. Available at: https://www.researchgate.net/publication/228676698%0D
[38] Bradshaw, J.M., Carvalho, M., Bunch, L., Eskridge, T., Feltovich, P.J., Johnson, M., et al., Sol: An Agent-Based Framework for Cyber Situation Awareness. KI - Künstliche Intelligenz, 26(2), pp. 127-140, 2012. DOI: https://doi.org/10.1007/s13218-012-0179-2
[39] Pastrana, S., Tapiador, J.E., Orfila, A., and Peris-Lopez, P., DEFIDNET: a framework for optimal allocation of cyberdefenses in intrusion detection Networks. Comput Networks. 80, pp. 66–88, 2015. DOI: https://doi.org/10.1016/j.comnet.2015.01.012
[40] Bodeau, D.J., Mccollum, C.D., and Fox, D.B., Cyber wargaming: framework for enhancing cyber wargaming with realistic business context [online]. Mc Lean, Virginia, USA, 2018. Available at: http://www.mitre.org/HSSEDI
[41] Katsantonis, N.M., Kotini, I., Fouliras, P., and Mavridis, I., Conceptual framework for developing cyber security serious games. In: IEEE Global Engineering Education Conference, EDUCON. IEEE Computer Society, 2019, pp. 872–81.
[42] Norman, M.D., and Koehler, M.T.K., Cyber defense as a complex adaptive system: a model-based approach to strategic policy design. In: Proceedings of the 2017 International Conference of The Computational Social Science Society of the Americas, 2017, pp. 1-7.
[43] Liu, S.Z., Li, Y.F., and Yang, Z., Modelling of cyber-attacks and defenses in local metering system. Energy Procedia. 145, pp. 421–426, 2018. DOI: https://doi.org/10.1016/j.egypro.2018.04.069
[44] Boyu, G.,and Libao, S., Modeling an attack-mitigation dynamic game-theoretic scheme for security vulnerability analysis in a cyber-physical power system. IEEE Access, 20, art. 2973030, 2020. DOI: https://doi.org/10.1109/ACCESS.2020.2973030
[45] Hasan, S., Dubey, A., Karsai, G., and Koutsoukos, X., A game-theoretic approach for power systems defense against dynamic cyber-attacks. Int J Electr Power Energy Syst. 115, art. 105432, 2020. DOI: https://doi.org/10.1016/j.ijepes.2019.105432
[46] Zeng, W., and Germanos, V., Modelling hybrid cyber kill chain, [online]. 2019. [cited: 2020. Oct 14th]. Available at: https://www.lockheedmartin.com
[47] Maathuis, C., Pieters, W., and Van den Berg, J., Decision support model for effects estimation and proportionality assessment for targeting in cyber operations. Defence Technology, 17(2), pp. 352-374, 2020. DOI: https://doi.org/10.1016/j.dt.2020.04.007
[48] Jacq, O., Brosset, D., Kermarrec, Y., and Simonin, J., Cyber-attacks real time detection: towards a cyber situational awareness for naval systems. In: *Cyber SA 2019*: International Conference on Cyber Situational Awareness, Data Analytics and Assessment, Oxford, United Kingdom, 2019. DOI: https://doi.org/10.1109/CyberSA.2019.8899351
[49] Pitropakis, N., Logothetis, M., Andrienko, G., Stefanatos, J., Karapistoli, E., and Lambrinoudakis, C., Towards the creation of a threat intelligence framework for maritime infrastructures. In: Katsikas, S., et al. Computer Security. CyberICPS SECPRE SPOSE ADIoT 2019 2019 2019 2019. Lecture Notes in Computer Science, vol 11980. Springer, Cham., 2020. DOI: https://doi.org/10.1007/978-3-030-42048-2_4
[50] Caselles-Moncho, A., Modelización y simulación de sistemas complejos. Tesis de grado, Universidad de Valencia, Valencia, España, 2008, 134 P.
[51] Izquierdo, L., Galan, J., Santos, J. y Del Olmo, R., Modelado de sistemas complejos mediante simulacion basada en agentes y dinámica de sistemas. Empiria Rev Metodol Ciencias Soc. 16, pp. 85–112, 2008.
[52] Siegfried, R., Modeling and simulation of complex systems. Springer Fachmedien Wiesbaden, München, 2014, 233, P.
[53] Sargent, R.G., Verification and validation of simulation models. In: Proceedings of the 2011 Winter Simulation Conference, 2011, pp. 83-98. DOI: https://doi.org/10.1109/WSC.2010.5679166
[54] Cabuya-Padilla, D.E., and Castaneda-Marroquin, C., Maritime cyberdefense actors taxonomy for command and control. In: Smart Innovation Systems and Technologies. United Kingdom, 2022, pp. 37-46.
[55] Alba-Rocha, D.A., Ortegon-Vega, J.R., Cabuya-Padilla, D.E., Riola-Rodríguez, J.M. y Fajardo-Toro, C.H., Modelo conceptual del sistema del poder marítimo a nivel estratégico en Colombia. RISTI - Rev Iber Sist e Tecnol Inf. 49, pp. 211–221, 2022.
[56] Buffa, B.A, Métodos matemáticos para modelos basados en agentes. Universidad Nacional de Córdoba, Córdoba, Argentina, 2015, 39 P.
[57] Schervish, M.J., Review of Simulation Modeling and Analysis., by Law, A.M., and Kelton, W.D., Journal of the American Statistical Association, 78(383), pp. 743–744, 1983. DOI: https://doi.org/10.2307/2288169
[58] Abar, S., Theodoropoulos, G.K., Lemarinier, P., and O'Hare, G.M.P., Agent based modelling and simulation tools: a review of the state-of-art software. Computer Science Review. 24, pp. 13-33, 2017. DOI: https://doi.org/10.1016/j.cosrev.2017.03.001
[59] Python Software Foundation. Python [online]. 2023. Available at: https://www.python.org/
[60] Weiner, M.G., War Gaming Methodology [online]. 1959. [cited: 2020, Sep 18th]. Available at: https://www.rand.org/content/dam/rand/pubs/research_memoranda/2008/RM2413.pdf
[61] Burns, S., Della-Volpe, D., Babb, R., Miller, N., and Muir, G., War Gamers' Handbook - A guide for professional war gamers. War Gaming Department, U.S. Naval War College, 2013.
[62] Maldonado, C.E., Gómez-Cruz, N.A., Modelamiento y simulación de sistemas complejos. Universidad del Rosario; Bogotá, Colombia, pp. 1-32, 2010.

D.E. Cabuya-Padilla, es Capitán de Corbeta de la Armada de Colombia. Ing. Electrónico, Administrador de Empresas, Profesional en Ciencias Navales, MSc. en Logística, MSc. en Gestión de la Información y estudiante del Doctorado en Ciencias del Mar. Con 8 años de experiencia docente e investigativa. Clasificado como Investigador Asociado por MinCiencias.
ORCID: 0000-0001-5338-9943

C.A. Castaneda-Marroquin, es Dr. en Informática y Telecomunicaciones de la Universidad Autónoma de Madrid, España, con un M.B.A. de IE Business School, España. Ha trabajado por más de 20 años en empresas en el área de ciberseguridad y Cloud Computing en Colombia y España. Docente e investigador en instituciones de educación superior en Colombia.
ORCID: 0000-0002-4957-158X