Sistema De Gestión De Riesgos Dinámicos En Entornos Operacionales Multidominio

Sánchez-Zas, Carmen[1*]; Jover-Walsh, Oscar[1]; Solera-Cotanilla, Sonia[1]; Camacho Gil, Adrián[2]; Moyano González, Eduardo[2]; Larriva-Novo, Xavier[1]; Ceballos Romero, Carlos A.[2]; Villagrá, Víctor A.[1]

[1] ETSI Telecomunicación, Universidad Politécnica de Madrid (UPM), Av. Complutense 30, 28040. Madrid, España. carmen.szas@upm.es

[2] Indra Sistemas, S.A. (INDRA). Av. de Bruselas, 35, 28108. Alcobendas, Madrid, España. acamachogi@indra.es

* Autor principal: Sánchez-Zas, Carmen; carmen.szas@upm.es

Resumen: La presente contribución describe el diseño de un sistema de gestión de riesgos dinámicos, concebido para abordar los requisitos operacionales asociados a las Operaciones Multidominio (*Multi-Domain Operations*, MDO) y al concepto de Guerra Mosaico. Este trabajo expone la necesidad de nuevas capacidades en el ámbito de la defensa para hacer frente a la creciente complejidad de los entornos operacionales modernos, caracterizados por la interacción simultánea entre los dominios terrestre, marítimo, aéreo, del espacio y ciberespacio. En este contexto, la conciencia cibersituacional y la gestión del riesgo emergen como elementos estratégicos clave para asegurar la continuidad de la misión y mantener la superioridad en la toma de decisiones. En escenarios multidominio, el riesgo debe entenderse como un fenómeno que surge de la interacción entre amenazas, vulnerabilidades y activos críticos. En la siguiente sección, se especifica detalladamente la propuesta y el diseño de un marco interoperable y se presenta una descripción a alto nivel del sistema, orientado a la monitorización continua de amenazas, la evaluación correlacional de riesgos y la priorización de mitigaciones en función de la criticidad y propagación de impactos que puedan afectar a los objetivos de la misión. Finalmente, se incluye un ejemplo de caso de estudio de un escenario de MDO con una misión estructurada en tres líneas de operación (Lines of Operation, LoO) [1]. Para esta prueba de concepto se evalúan las diferentes tareas, cuyo cumplimiento permite alcanzar el objetivo de una de las líneas de operación. En este sentido, cabe destacar la capacidad del sistema para adaptarse a distintos enfoques doctrinales y ofrecer una visión consolidada del entorno de riesgo. El artículo concluye que el sistema de gestión de riesgos contribuiría significativamente a mejorar la conciencia cibersituacional, facilitando el soporte al Proceso Militar para la Toma de Decisiones y fomentando la interoperabilidad entre metodologías de gestión de riesgos.

Palabras clave: Conciencia Cibersituacional, Gestión de Riesgos, Guerra Mosaico, Mando y Control, Proceso Militar de Toma de Decisiones, Operaciones Multidominio.

1. Introducción

La creciente complejidad de los entornos operacionales modernos, caracterizados por la interacción simultánea de múltiples dominios (tierra, mar, aire, espacio y ciberespacio), exige el desarrollo de nuevas capacidades que garanticen la continuidad de la misión en escenarios altamente dinámicos y disputados [2], [3], [4]. La Organización del Tratado del Atlántico Norte (OTAN) define las MDO como «la orquestación de actividades militares, en todos los dominios y entornos, sincronizadas con actividades no militares, para permitir a la Alianza crear efectos convergentes a la velocidad pertinente» [5]. En este contexto, las MDO y la Guerra Mosaico representan un cambio doctrinal [6], [7]: fuerzas distribuidas, interconectadas y adaptables que actúan de forma sincronizada para generar efectos decisivos.

Uno de los desafíos críticos en estos escenarios es la gestión del riesgo [8], [9]. En el ámbito militar, el riesgo no puede ser abordado como una amenaza puntual o aislada, sino como un fenómeno dinámico derivado de la interacción entre múltiples factores [10]: vulnerabilidades de sistemas, activos críticos y capacidades hostiles. Comprender y gestionar estos riesgos en tiempo real es esencial para la continuidad operativa y la toma de decisiones.

Como respuesta, se propone un sistema de gestión de riesgos dinámicos orientado a MDO capaz de monitorizar en tiempo real el estado de amenazas, vulnerabilidades y activos críticos distribuidos en distintos niveles y dominios. Más allá de una simple evaluación de riesgos, el sistema permite identificar dependencias, anticipar la propagación de riesgos y priorizar medidas de mitigación.

2. Propuesta

2.1 Metodología

El sistema propuesto parte de la necesidad de adaptar los enfoques tradicionales de análisis de riesgos a las demandas específicas del entorno multidominio [8]. Para ello, se plantea una metodología que combina estándares de gestión de riesgos existentes en marcos normativos nacionales y europeos, identificando áreas de convergencia que faciliten un marco común e interoperable, el diseño de una arquitectura funcional, y la validación del sistema en escenarios simulados.

2.2 Diseño Funcional del Sistema de Gestión de Riesgos en Entornos Multidominio

La Figura 1 presenta la propuesta de un marco para llevar a cabo procesos de gestión dinámica de riesgos en entornos de MDO. En primer lugar, es imprescindible identificar y modelar los conceptos clave asociados a la gestión de riesgos de ciberseguridad, entre los que se incluyen incidente, activo, amenaza y riesgo potencial y residual. Asimismo, es necesario incorporar conceptos propios de los entornos de MDO [1], [11], tales como: Misión (Mission), Tarea (Task), LoO, Efecto (Effect), y Objetivo (Objective).

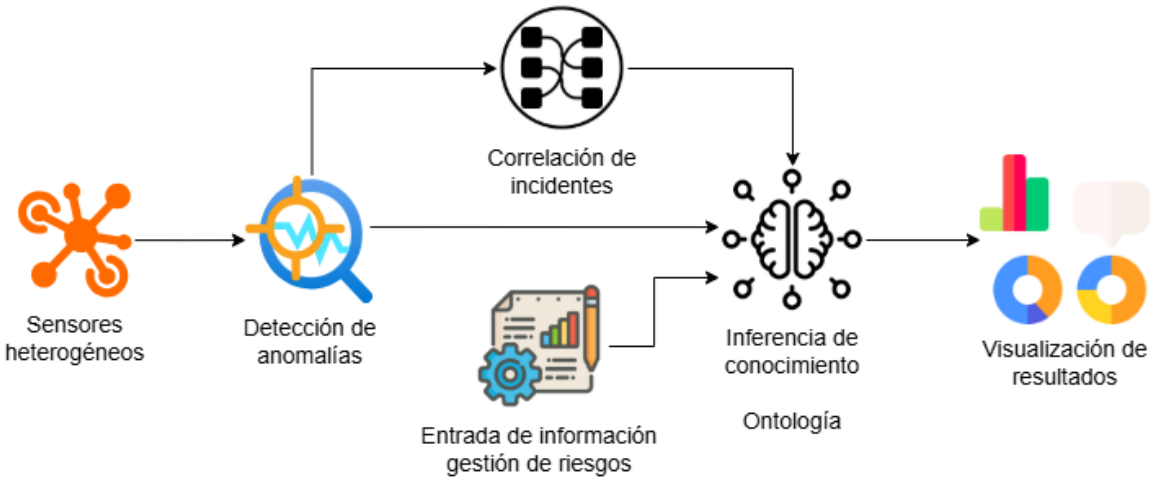

Figura 1. Estructura de la propuesta para un sistema dinámico gestión de riesgos.

Para el proceso de identificación, análisis y evaluación de riesgos se parte de la propuesta presentada en [12], adaptándola al entorno MDO. Para el proceso de identificación, análisis y evaluación de riesgos se parte de la propuesta presentada en [12], adaptándola al entorno MDO. El sistema comienza con la ingesta de registros provenientes de **sensores** y dispositivos heterogéneos desplegados en los distintos dominios operacionales. La detección de uno o varios **incidentes** correlados de ciberseguridad que afectan a uno o más **activos** genera una **amenaza**, desencadenando en un **riesgo** (R), definido como la combinación de la probabilidad de ocurrencia (P) y el nivel de impacto (I) resultando en ($R = P \times I$). Este riesgo implica una disminución del valor del activo en una o más dimensiones de la ciberseguridad: Confidencialidad (Confidenciality, C), Integridad (Integrity, I), Disponibilidad (Availability, A), etc.

Dicha información se recoge en una ontología formalizada, diseñada para inferir autom áticamente los resultados del proceso de gestión de riesgos a partir de los datos de entrada y un conjunto de escenarios de amenaza. Posteriormente, el sistema evalúa el impacto potencial del riesgo en función de la relación del activo comprometido con las líneas de operación de la misión. Si el impacto afecta la ejecución de tareas clave, se incrementa la

probabilidad de que la línea de operación no alcance sus objetivos, comprometiendo así el desarrollo global de la misión.

3. Caso de estudio

Para validar el sistema, se plantea una prueba de concepto basada en un escenario de MDO. En este escenario, la misión se estructura en tres líneas de operación: tierra, aire y mar. El objetivo operativo de la última línea de operación es asegurar la navegación en un estrecho para permitir el flujo de recursos hacia una zona de conflicto. Para ello, debe alcanzarse una condición decisiva: la neutralización de amenazas que comprometan dicho espacio marítimo. Con este propósito, se identifican cuatro tareas defensivas clave: (1) establecer vigilancia continua sobre el tráfico marítimo, (2) proteger la línea de comunicaciones navales frente a posibles actos de sabotaje, (3) proporcionar cobertura aérea en la zona de operaciones, y (4) mantener la superioridad en los dominios naval e informacional. Para el cumplimiento de esta última tarea, se dispone de un Centro de Mando y Control embarcado, capaz de respaldar la toma de decisiones mediante el análisis de datos confiables en tiempo real. Este escenario se presenta en la Tabla 1.

	Condiciones
LoO Terrestre	30 % sobre el éxito de la misión
LoO Aérea	30 % sobre el éxito de la misión
LoO Naval	40 % sobre el éxito de la misión
↳ Condición Decisiva (CD) LoO Naval	100 % sobre el éxito de LoO Naval Mínimo éxito de CD requerido: 75%
↳ Efecto 1	20 % sobre el éxito de CD
| ↳Tarea 1: Vigilancia tráfico	100 % sobre el éxito de Efecto 1
↳ Efecto 2	20 % sobre el éxito de CD
| ↳Tarea 2: Proteger comunicación	100 % sobre el éxito de Efecto 2
↳ Efecto 3	30% sobre el éxito de CD
| ↳Tarea 3: Cobertura aérea	100 % sobre el éxito de Efecto 3
↳ Efecto 4	30% sobre el éxito de CD
↳Tarea 4: Superioridad Naval e Informacional	100 % sobre el éxito de Efecto 4 Mínimos valores CIA: (2,6,4)
↳ Activo: Centro de Mando y Control	Valores CIA originales: (8,6,7)

Tabla 1. Caso de estudio – Estado inicial

Cuando el modelo de detección de anomalías identifica que el centro de inteligencia está siendo objeto de un ataque, el sistema de gestión de riesgos dinámicos asigna automáticamente una amenaza potencial de modificación de los datos de los sensores, con

una probabilidad media y un impacto muy alto. En función de este impacto se reduce la valoración del activo principal en la dimensión de integridad en un 50%.

A continuación, se evalúa cómo la pérdida de integridad compromete el éxito de la misión en la línea de operación afectada. En este caso, la tarea de mantener la superioridad en el estrecho depende críticamente de la integridad de los datos analizados. Como el valor del activo no alcanza el umbral requerido, solo la tarea 4 se considera fallida. Sin embargo, la imposibilidad de cumplir esta tarea impide alcanzar la condición decisiva (neutralización de amenazas en el área), lo que compromete el cumplimiento del objetivo operativo. Además, la ejecución de la tarea en condiciones degradadas podría incrementar la probabilidad de efectos colaterales no deseados, como descoordinación entre unidades, fuego amigo, uso ineficiente de recursos o exposición de otros activos críticos. En la Tabla 2 se representan en rojo las condiciones que no se cumplen.

	Éxito	**Condiciones**
Misión	**60 %**	
LoO Terrestre (30 % sobre la misión)	100 %	
LoO Aérea (30 % sobre la misión)	100 %	
LoO Naval (40 % sobre la misión)	0%	
↳ **CD** (100 % sobre LoO Naval)	70 %	Mínimo éxito de CD requerido: 75%
↳ **Efecto deseado 1** (20 % sobre CD)	100 %	
| ↳**Tarea 1** (100 % sobre Efecto 1)	100 %	
↳ **Efecto deseado 2** (20 % sobre CD)	100 %	
| ↳**Tarea 2** (100 % sobre Efecto 2)	100 %	
↳ **Efecto deseado 3** (30 % sobre CD)	100 %	
| ↳**Tarea 3** (100 % sobre Efecto 3)	100 %	
↳ **Efecto deseado 4** (30 % sobre CD)	0 %	
↳ **Tarea 4** (100 % sobre Efecto 4)	0 %	Mínimos valores CIA: (2,6,4)
↳ **Centro de Mando y Control**	-	Valores CIA finales: (8,6,3.5)

Tabla 2. Caso de estudio – Estado Final

4. Conclusiones

El presente artículo expone la necesidad urgente de soluciones enfocadas a fortalecer la conciencia cibersituacional y apoyar el Proceso Militar para la Toma de Decisión en entornos multidominio [13]. Como respuesta, se propone un sistema dinámico de gestión de riesgos,

interoperable y orientado a la detección temprana e identificación en tiempo real de anomalías, vulnerabilidades, activos críticos y capacidades hostiles que puedan comprometer el entorno operacional.

Se evalúa la propuesta del sistema mediante un caso de estudio que analiza una situación crítica de un entorno multidominio donde el incumplimiento de las tareas de cada línea de operación pone en riesgo el cumplimiento y ejecución de la misión. Esta prueba de concepto expone la mejora de la conciencia cibersituacional que ofrece el sistema propuesto, posicionándolo como un recurso clave en operaciones conjuntas dentro del marco multidominio del combate moderno.

Referencias

[1] 'NATO STANDARD. AJP-5 ALLIED JOINT DOCTRINE FOR THE PLANNING OF OPERATIONS. Edition A Version 2', 2019.

[2] Fernando Carrillo Cremades, Fernando Luis Morón Ruiz, Luis Francisco Astorga González, Manuel Buesa Bueno, Rubén Vega Bustelo, and Juan Ramón González Espadas, 'Transformación digital de las FAS para el combate multidominio', 2023.

[3] B. Liljedahl, J. Runesson, and F. C. W. S. Tamm, 'Multi-Domain Operations (MDO) Facing a Complex Reality', 2025.

[4] I. C. Manolache, 'The Role of Multi-Domain Operations in Modern Warfare', *Land Forces Academy Review*, vol. 28, no. 3, pp. 163–170, Sep. 2023, doi: 10.2478/raft-2023-0020.

[5] F. D. Kramer, A. M. Dailey, and J. A. Brodfuehrer, 'NATO multidomain operations Near-and medium-term priority initiatives', 2024.

[6] G. Pulido, Guerra multidominio y mosaico: el nuevo pensamiento militar estadounidense. Los libros de la Catarata, 2022.

[7] J. Jordán, 'Guerra Mosaico: Qué Es y A Qué Desafíos Se Enfrenta', 2023.

[8] M. Jeremy Phillips, 'Risk Perception in Multi-Domain Operations', 2021.

[9] David S. Alberts, 'Agile Multi-Domain Command and Control. Key to Managing Cyber Risk to Mission', 2020. [Online]. Available: https://media.defense.gov/2018/Sep/18/2002041658/-1/1/1/CYBER_STRATEGY

[10] Á. L. Martínez, J. M. Vidal, and V. A. V. González, 'Understanding and Assessment of Mission-Centric Key Cyber Terrains for joint Military Operations', Nov. 2021, [Online]. Available: http://arxiv.org/abs/2111.07005

[11] 'DOD Dictionary of Military and Associated Terms', 2017. [Online]. Available: http://www.dtic.mil/doctrine/dod_dictionary

[12] C. Sánchez-Zas, X. Larriva-Novo, V. A. Villagrá, D. Rivera, and A. Marín-Lopez, 'A methodology for ontology-based interoperability of dynamic risk assessment frameworks in IoT environments', *Internet of Things (Netherlands)*, vol. 27, Oct. 2024, doi: 10.1016/j.iot.2024.101267.

[13] O. técnico, R. M. Ryder, and C. de Reserva del Ejército de EUA, 'La superioridad de conciencia de dominios es el futuro de la inteligencia militar', 2022.