ECySAP y la conciencia situacional en operaciones de guerra multidominio

Antonio Legaz
Juan Tejero
José Francisco Suárez Mulero

Resumen

El artículo analiza el papel de ECySAP (Enhanced Cyber Situational Awareness Platform) como plataforma integral para la generación de conciencia situacional cibernética (CySA) en el contexto de operaciones militares multidominio. A partir de una evolución conceptual desde el «coup d'œil» de Clausewitz hasta el modelo de Endsley adaptado al ciberespacio, se expone cómo ECySAP permite percibir, comprender y proyectar amenazas en entornos complejos, facilitando la toma de decisiones, la planificación operativa y la gestión de riesgos. Se detalla su arquitectura funcional, su potencial integración con inteligencia artificial y su papel como habilitador de la guerra mosaico, donde la interoperabilidad y la sincronización entre dominios son clave. A través de un caso de uso hipotético basado en la anexión de Crimea, se ilustra cómo ECySAP podría haber contribuido a mitigar riesgos, detectar campañas de desinformación y proteger infraestructuras críticas, alineándose con doctrinas OTAN y marcos normativos europeos.

Palabras clave

Conciencia situacional, Guerra multidominio, Guerra mosaico, Ciberdefensa, Inteligencia artificial.

ECySAP and situational awareness in multi-domain warfare operations

Abstract

The article analyzes the role of ECySAP (Enhanced Cyber Situational Awareness Platform) as an integral platform for cyber situational awareness generation (CySA) in the context of multi-domain military operations. Based on a conceptual evolution from the "coup d'œil" of Clausewitz to the Endsley model adapted to cyberspace, it is exposed how ECySAP allows to perceive, understand and project threats in complex environments, facilitating decision making, operational planning and risk management. It details its functional architecture, its potential integration with artificial intelligence and its role as enabler of mosaic

warfare, where interoperability and cross-domain synchronization are key. Through a hypothetical use case based on the annexation of Crimea, it illustrates how ECySAP could have contributed to mitigating risks, detecting disinformation campaigns and protecting critical infrastructure by aligning with NATO doctrines and European regulatory frameworks.

Keywords

Situational Awareness, Multidomain Operations, Network-Centric Warfare, Cyberdefence, Artificial Intelligence.

1 Fundamentos de la Conciencia Situacional Cibernética (CySA)

1.1 Del Coup d'Oeil a la Conciencia Situacional Cibernética: transformación del paradigma militar

El concepto de «coup d'œil», definido por Carl von Clausewitz, hace referencia a la capacidad de un líder para percibir de manera intuitiva y rápida la verdad en una situación compleja. Clausewitz describía esta acción como un ejercicio basado en el instinto y la sensación de la verdad, sin apoyo en datos cuantificables o en análisis extensivos. En el contexto de los campos de batalla tradicionales, caracterizados por una estructura lineal y una relativa claridad en las operaciones, la intuición combinada con el discernimiento y la previsión permitía a los comandantes tomar decisiones oportunas y efectivas. Sin embargo, la naturaleza del conflicto ha evolucionado de manera drástica con la irrupción del dominio cibernético, el cual ha redefinido los métodos y desafíos de la toma de decisiones.

El actual entorno cibernético se caracteriza por su complejidad, dinamicidad y alto grado de incertidumbre. A diferencia de los conflictos tradicionales, este dominio se ve marcado por la interconexión global, la rapidez de los acontecimientos y la multiplicidad de actores involucrados, lo que limita la efectividad de una toma de decisiones basada exclusivamente en la intuición individual. La toma de decisiones en el ciberespacio se enfrenta a una «niebla de guerra» más densa que nunca, donde las amenazas evolucionan rápido y los adversarios utilizan tácticas cada vez más sofisticadas. En este contexto, la Conciencia Situacional Cibernética (Cyber Situational Awareness, CySA) surge como una necesidad imperativa para comprender y actuar de manera eficaz en este escenario.

1.2 Evolución histórica de la conciencia situacional: de Sun Tzu al entorno digital

El concepto de conciencia situacional ha adquirido una relevancia fundamental en múltiples disciplinas, en especial, en el ámbito militar. Aunque el término es relativamente reciente, la esencia de esta capacidad cognitiva, es decir, la percepción, comprensión y proyección del entorno para una toma de decisiones efectiva, ha sido reconocida y aplicada en la estrategia y táctica militar desde tiempos antiguos.

Desde la antigüedad, los líderes militares han reconocido la importancia de una percepción clara del entorno para la planificación y ejecución de operaciones. En *El arte de la guerra*, escrito por Sun Tzu en el siglo v a. C., se enfatiza la necesidad de conocer tanto al enemigo como a uno mismo como un principio esencial para la victoria. La afirmación «Si conoces al enemigo y te conoces a ti mismo, no debes temer el resultado de cien batallas» ilustra

una concepción temprana de la conciencia situacional, basada en la comprensión del contexto y la anticipación de las acciones del adversario.

En los siglos XVIII y XIX, la literatura militar europea reflejaba esta misma preocupación por la percepción del entorno. En los tratados de estrategia de la época napoleónica, se destacaba la relevancia del reconocimiento del terreno, la observación de las condiciones climáticas y la recopilación de información sobre la disposición enemiga. Durante las campañas de Napoleón Bonaparte, por ejemplo, el uso de exploradores y unidades de reconocimiento permitió a los comandantes adaptar sus estrategias en función de información actualizada, demostrando una comprensión implícita de lo que hoy se denomina conciencia situacional.

Con la Primera Guerra Mundial, el concepto evolucionó en el ámbito aéreo. El término «situational awareness» comenzó a emplearse para describir la capacidad de los pilotos de combate para mantenerse conscientes de su entorno y de los movimientos enemigos, una habilidad crucial para la supervivencia en el combate aéreo. Posteriormente, en conflictos como la guerra de Corea y la guerra de Vietnam, los pilotos de la Fuerza Aérea de los Estados Unidos identificaron esta capacidad como el «factor as» (ace factor), es decir, la aptitud para anticipar y reaccionar de manera eficaz ante maniobras adversarias.

1.3 Marco teórico de la Conciencia Situacional Cibernética: el modelo de Endsley en el Ciberespacio

La Conciencia Situacional (SA) se define como la percepción de elementos en el entorno dentro de un volumen de tiempo y espacio, la comprensión de su significado y la proyección de su estado en un futuro próximo (Endsley, 1988). Este concepto ha experimentado una evolución natural hacia el dominio cibernético. La Conciencia Situacional Cibernética (CySA) surge como respuesta a la necesidad de aplicar estos principios al complejo entorno digital contemporáneo, caracterizado por amenazas difusas y en constante evolución (Franke y Brynielsson, 2014).

La adaptación de este concepto al ámbito cibernético no ha sido trivial. Mientras que en entornos físicos la percepción se realiza, principalmente, a través de los sentidos humanos, en el ciberespacio esta percepción depende, sobre todo, de sistemas técnicos y herramientas de monitorización (Barford *et al*., 2010). Esta transición conceptual ha requerido un replanteamiento de los modelos clásicos para incorporar las particularidades del entorno digital.

El modelo de Endsley, ampliamente reconocido, establece tres niveles jerárquicos para la CySA. El primer nivel, la percepción, implica la recopilación de datos del entorno cibernético mediante sensores, dispositivos de monitorización y sistemas de detección de intrusiones (Endsley y Connors,

2008). Esta fase resulta crucial, pues constituye la base informativa sobre la que se construye toda comprensión posterior del escenario cibernético.

El segundo nivel, la comprensión, conlleva el análisis e interpretación de los datos recopilados para formar una imagen coherente de la situación actual. Este proceso requiere no solo capacidades técnicas, sino también contextualización y correlación de eventos, en apariencia, dispares para identificar patrones significativos (Tadda y Salerno, 2010). La comprensión adecuada permite discriminar entre falsos positivos y amenazas reales, optimizando así la asignación de recursos defensivos.

Finalmente, el tercer nivel, la proyección, representa la capacidad para anticipar la evolución futura del escenario cibernético basándose en la comprensión actual de la situación (Onwubiko, 2016). Esta capacidad predictiva resulta fundamental para la planificación estratégica y la implementación proactiva de medidas defensivas antes de que las amenazas potenciales se materialicen.

La relación de la CySA con el concepto de *ground truth* es intrínseca y complementaria. El *ground truth* representa la realidad objetiva del entorno cibernético, con independencia de las limitaciones perceptivas o interpretativas de los analistas (Jajodia *et al*., 2010). Lograr una conciencia situacional efectiva implica aproximarse lo máximo posible a esta verdad fundamental, reconociendo que la complejidad del ciberespacio impone limitaciones inherentes a esta aspiración (McGuinness y Foy, 2000).

1.4 Contexto operativo contemporáneo: guerra multidominio y enfoque mosaico

Las guerras modernas ya no se tratan solo de tener la mayor potencia de fuego o el mejor blindaje, sino también de tener una superior conciencia situacional, la capacidad de procesar información rápidamente y de tomar decisiones más rápido que el oponente (Pulido, 2021). El concepto del ciclo OODA (Observar, Orientar, Decidir y Actuar) se ha vuelto fundamental en la planificación y ejecución de las operaciones militares (Boyd, 1976). Este ciclo destaca por la importancia de la velocidad y la agilidad en la toma de decisiones para obtener una ventaja en el campo de batalla.

La transición hacia las operaciones multidominio surge de la necesidad de los ejércitos de ser capaces de operar simultáneamente en todos estos dominios, reconociendo que las acciones en uno de ellos pueden tener efectos en cascada en los demás (Fojon, 2020). Las operaciones multidominio no se limitan al conflicto armado, sino que abarcan una visión más holística de la estrategia militar. Esto implica la necesidad de coordinar los esfuerzos en diferentes dimensiones, como lo terrestre, marítimo, aéreo, ciberespacial, aeroespacial y el espectro electromagnético.

Esta necesidad de coordinación y de operar en un entorno complejo ha dado lugar al concepto de guerra mosaico, que se basa en la idea de que las grandes plataformas militares pueden ser divididas en una serie de funciones que pueden ser llevadas a cabo por componentes individuales, pero interconectados (Jordán, 2023). Cada uno de estos componentes equivaldría a una pieza de un mosaico, operando en conjunto para lograr un objetivo común. De esta manera, la guerra mosaico busca superar las limitaciones de los sistemas monolíticos y crear una fuerza de combate más adaptable y flexible.

La guerra mosaico se caracteriza por la desagregación de funciones, donde los sensores, los responsables de la toma de decisiones y los ejecutores de acciones se convierten en entidades separadas que se comunican y colaboran en una red (Pulido, 2021). La importancia de la información y la conectividad en este nuevo paradigma es central, pues todos los «tiradores» deben ser capaces de usar la información de todos los sensores, creando una «red de muerte» o «kill web» (López Díaz, 2020). Esta arquitectura no jerárquica y distribuida permite una mayor capacidad de adaptación y resiliencia.

2 ECySAP: plataforma integral para la Conciencia Situacional Cibernética

ECySAP funciona como una plataforma integrada y modular que facilita el traslado de información sobre incidentes, amenazas, riesgos e impactos en el plano cibernético, a los diferentes efectos y objetivos de las misiones. Esto se alinea con el concepto de un Cyber Common Operational Picture (CyCOP), cuyo objetivo es integrar y contextualizar numerosos flujos de datos y puntos de datos para acelerar la conciencia situacional cibernética (Kim *et al*., 2023: 1).

Esta herramienta integral de apoyo al planeamiento y misión multisectorial permite que la información generada se integre de manera efectiva en los procesos de planificación, optimizando la rapidez y precisión en la toma de decisiones (Indra, 2021). La conciencia situacional (SA), aunque ligada a la cognición humana, es esencial para percibir el entorno (Schaberreiter *et al*., 2022: 149, citado en Kim *et al*., 2023: 2) y ECySAP contribuye de manera significativa a este propósito.

Dado el creciente nivel de interdependencia entre dominios físicos y digitales, las operaciones militares y de seguridad deben adoptar un enfoque holístico para lograr una representación precisa del entorno operativo. ECySAP no solo se enfoca en la identificación y mitigación de riesgos cibernéticos, sino que también facilita el análisis, la identificación y validación de elementos clave en múltiples dominios operativos.

2.1 Arquitectura funcional de ECySAP: de la percepción a la proyección

ECySAP se fundamenta en una arquitectura de múltiples niveles diseñada para optimizar la toma de decisiones en entornos operacionales complejos. La estructura de esta se organiza en dos capas principales (figura 1):

— Capa de Misión o *Mission Layer*: incluye los objetivos y tareas de misión, representando el nivel estratégico y táctico de la operación.

— Capa de Sistemas de Información y Comunicación o *CIS Layer*: contiene los servicios y sistemas CIS, responsables de proporcionar la infraestructura tecnológica necesaria para el desarrollo de la misión.

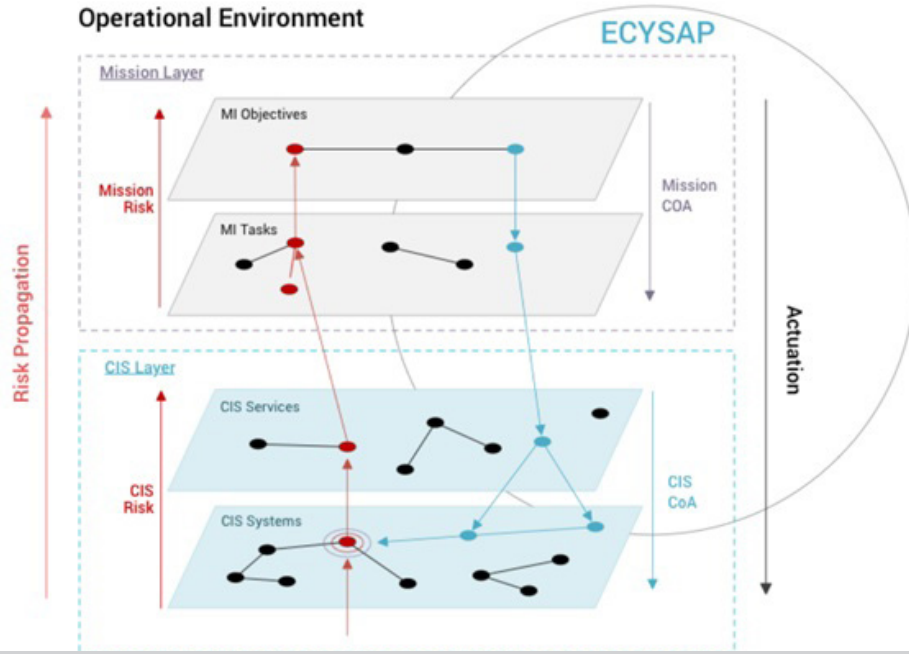

Figura 1. Fuente: ecysap.eu

Uno de los aspectos clave en la arquitectura del ECYSAP es la propagación del riesgo desde los sistemas CIS hasta los objetivos de misión. Los riesgos en la CIS Layer, originados en los CIS Systems y que afectan a los CIS Services, pueden propagarse hacia la Mission Layer, afectando las tareas y objetivos de la misión. Estos fallos o vulnerabilidades en los sistemas de información pueden comprometer servicios críticos, generando impactos adversos en la ejecución de tareas y en la consecución de los objetivos estratégicos.

Para mitigar estos riesgos, se aplican Cursos de Acción (CoA) en la capa de misión y en la capa CIS se recurre a contramedidas. ECySAP puede ayudar en la toma de decisiones para establecer un CoA óptimo, presentando la información de manera detallada tanto en el plano cibernético como en el de misión. De este modo, se facilita la gestión del riesgo y se refuerza la resiliencia operativa ante incidentes cibernéticos.

2.2 Aplicaciones de ECySAP en la planificación operativa y cursos de acción

La información que proporciona ECySAP sobre la materialización de amenazas e incidentes, riesgos e impactos y su repercusión en las misiones es fundamental para la toma de decisiones. Esta información sirve como una vital aportación para comprender la situación en el ciberespacio en términos de impacto (Comunicación Oficial Demostrador, 2025), lo cual es esencial para la planificación de misiones y la definición de Cursos de Acción (CoA), como se describe en el contexto del proceso de planificación operativa de la OTAN (NATO Allied Command Operations, 2010: 4-31).

La planificación operativa implica el análisis de la misión y el desarrollo de COA (NATO Allied Command Operations, 2010: 4-15). Un CyCOP, como el desarrollado por Universitat Politècnica de València, tiene como objetivo generar conciencia situacional cibernética híbrida (CyHSA), fusionando información del dominio cibernético con información georreferenciada de sistemas de comando y control del dominio físico, proporcionando una visión integral para la toma de decisiones (Esteve *et al*., 2016).

ECySAP, al proporcionar información relevante sobre la situación cibernética, puede actuar como una base para la integración con sistemas de soporte a la decisión, permitiendo a los comandantes o responsables de misión desarrollar estrategias y tácticas en misiones de ciberdefensa en un espacio de toma de decisiones basado en una conciencia situacional precisa y adecuada.

Asimismo, esta plataforma desarrolla e implementa herramientas analíticas avanzadas para detectar y evaluar riesgos en el entorno tecnológico, analizando su posible propagación y el impacto sobre los objetivos operacionales. En un futuro, se plantea que el sistema pueda emplear técnicas sofisticadas para el intercambio de información sobre amenazas cibernéticas entre distintos actores, fortaleciendo sus capacidades individuales y colectivas de respuesta a través de la ejecución eficiente de estrategias durante la misión.

2.3 Gestión de riesgos y evaluación de incidentes a través de ECySAP

ECySAP, al proporcionar información clave sobre incidentes, amenazas, riesgos y su impacto en las misiones, facilita y ofrece funcionalidades para

el análisis de riesgos y la evaluación de las consecuencias de los incidentes (Llopis y López, 2024). Este enfoque responde a la necesidad de evaluar el daño de los ataques cibernéticos (Kim *et al*., 2022: 59270-59276, citado en Kim *et al*., 2023) y va más allá de la simple identificación de incidentes, permitiendo una comprensión profunda del contexto operacional en el que se desarrollan las capacidades de los sistemas de información y su impacto en las misiones (NATO Standardization Office, 2024: A-3).

En este sentido, el concepto de conciencia del riesgo situacional cobra relevancia, ya que busca evaluar las amenazas y vulnerabilidades de sistemas sociotécnicos complejos (Chatzimichailidou *et al*., 2015, citado en Kim *et al*., 2023: 6).

Para abordar este análisis de manera estructurada, ECySAP sigue una serie de pasos clave en la evaluación de riesgos y consecuencias:

1. Identificación de activos críticos: se determinan los elementos esenciales, como servidores y firewalls, y su relación con la misión.
2. Evaluación de riesgos y vulnerabilidades: se analizan amenazas mediante métricas cuantitativas, considerando tanto el contexto técnico como el operativo y la misión en curso.
3. Análisis de resiliencia cibernética: ECySAP proporciona los datos en bruto necesarios para que el analista examine la capacidad de los sistemas para resistir ataques y minimizar su impacto.
4. Evaluación del impacto en la misión: se proyectan escenarios para optimizar la toma de decisiones en distintos niveles operacionales.

Este enfoque integral permite a ECySAP proporcionar información relevante en entornos militares, facilitando la planificación de misiones y la definición de cursos de acción (U.S. Army, 2023). Un caso concreto de este proceso sería la identificación de un servidor de correo como un activo crítico para la comunicación en una operación militar. En este escenario, la evaluación no solo contemplaría la vulnerabilidad técnica del servidor ante ataques de denegación de servicio, sino también el impacto que la interrupción de las comunicaciones podría tener en el éxito de la misión (Documento interno, 2024).

2.4 Integración de inteligencia artificial: potenciando las capacidades de ECySAP

La inteligencia artificial (IA) se considera una herramienta clave para mejorar la toma de decisiones, pues permite analizar grandes volúmenes de datos con rapidez, proporcionar soporte dinámico a los decisores y generar propuestas estratégicas (Llopis y López, 2024). En este sentido, la IA facilita la visualización de información al refinar automáticamente las

representaciones en función de los niveles de riesgo, lo que mejora la comprensión de situaciones complejas (Llopis, 2023).

Uno de los principales usos de la IA es la automatización de la detección de *malware* y la gestión de incidentes. Algoritmos de aprendizaje automático, como Ensemble Machine Learning y Self-Adjusting Memory k-Nearest Neighbors, permiten analizar flujos de datos en tiempo real para identificar patrones maliciosos (Llopis, Esteve y Mees, 2023). Estos sistemas pueden detectar comportamientos anómalos que indiquen una infección o un ataque en curso, permitiendo una respuesta rápida y eficiente. Además, la automatización reduce la carga de trabajo de los analistas, liberándolos para tareas más complejas, mientras que los sistemas basados en IA pueden aplicar contramedidas de forma automática, como el bloqueo de direcciones IP maliciosas o el aislamiento de máquinas infectadas.

De igual manera, la IA se emplea para estudiar el comportamiento de los atacantes y elaborar perfiles de ciberataques, identificando las Tácticas, Técnicas y Procedimientos (TTPs) utilizados por grupos de ciberdelincuentes (U.S. Army, 2021). Esta capacidad facilita la anticipación y prevención de posibles amenazas. Además, la IA contribuye a la toma de decisiones en tiempo real al analizar de manera rápida grandes cantidades de datos, ofrece recomendaciones concretas y simula el impacto de diferentes estrategias, lo que permite a los comandantes tomar decisiones mejor fundamentadas.

En el contexto de ECySAP, la plataforma se beneficiará significativamente de la IA, en especial, a través de algoritmos de aprendizaje automático. En la actualidad, ECySAP no cuenta con IA integrada, pero se está desarrollando el proyecto ECySAP EYE para su futura implementación. Esta evolución permitirá a ECySAP mejorar de manera significativa su eficacia, al posibilitar un análisis más exhaustivo de los datos recopilados y transformar información bruta en inteligencia procesable para la toma de decisiones.

2.5 ECySAP en el contexto de la Guerra Mosaico: habilitador de Conciencia Situacional Multidominio

En el contexto de la guerra mosaico, la relación entre la plataforma ECySAP y las redes de efectos es fundamental para comprender la dinámica de las operaciones militares modernas. La guerra mosaico se caracteriza por la desagregación de fuerzas, la adaptabilidad y la creación de múltiples dilemas para el adversario, en lugar de depender de grandes plataformas monolíticas y la confrontación directa (López Díaz, 2020). En este marco, la plataforma ECySAP desempeña un papel crucial al habilitar la conciencia situacional necesaria para coordinar y sincronizar acciones en diferentes dominios, lo que a su vez permite la generación efectiva de redes de efectos (Maestre *et al*., 2022).

La plataforma ECySAP facilita esta visión integral al proporcionar una comprensión profunda del ciberespacio, un dominio que, en la guerra mosaico, tiene un impacto transversal en todos los demás. ECySAP integra información de diversas fuentes, incluyendo sensores físicos y lógicos, para construir una imagen completa de la situación operativa (Maestre *et al*., 2022). Esta capacidad de integración de información es fundamental para la creación de redes de efectos, ya que permite identificar las vulnerabilidades en el sistema del adversario y los puntos críticos que pueden ser explotados para generar el máximo impacto.

En este sentido, ECySAP no solo ofrece información sobre la actividad en el ciberespacio, sino que también permite comprender cómo dicha actividad afecta a otros dominios. Por ejemplo, un ataque cibernético coordinado puede degradar las comunicaciones del enemigo, interrumpir sus sistemas de mando y control, y afectar la precisión de sus armas guiadas, creando así un efecto dominó en otros dominios. Al proporcionar esta visión multidominio, ECySAP se convierte en un habilitador esencial para la planificación y ejecución de redes de efectos que busquen desarticular la capacidad del adversario.

2.6 ECySAP como habilitador de operaciones sincronizadas en entornos multidominio

La efectividad de las operaciones multidominio depende fundamentalmente de la capacidad para sincronizar acciones en diferentes espacios de batalla, generando efectos que se amplifican mutuamente. ECySAP trasciende su rol como mera plataforma de análisis cibernético para convertirse en un elemento vertebrador de la integración entre dominios (Maestre *et al*., 2022). Esta capacidad se materializa a través de diversas funcionalidades que facilitan la transición del paradigma tradicional de operaciones segmentadas hacia un enfoque verdaderamente integrado.

Una de las contribuciones más significativas de ECySAP a las operaciones multidominio es su capacidad para establecer correlaciones entre eventos cibernéticos y sus potenciales manifestaciones en otros dominios. Por ejemplo, la detección de actividades de reconocimiento en redes militares puede correlacionarse con datos de vigilancia electromagnética y movimientos de tropas, proporcionando indicadores tempranos de acciones inminentes en el dominio físico (López-Muñiz, 2023). Esta correlación multidimensional posibilita la identificación de patrones que permanecerían ocultos al analizar cada dominio de manera aislada.

La plataforma incorpora capacidades de análisis predictivo y simulación que permiten a los comandantes y estados mayores explorar escenarios sintéticos y anticipar efectos cruzados entre dominios. Estas funciones se

orientan a evaluar cómo incidentes en el ciberespacio -como ataques contra sistemas de control industrial (SCADA) o la degradación de servicios de posicionamiento satelital (GPS)- pueden impactar sobre la logística militar o la eficacia de sistemas de armas guiadas. Estos ejercicios contribuyen a desarrollar intuición operativa sobre las interdependencias entre dominios, preparando a los decisores para gestionar la complejidad inherente a las operaciones modernas.

Quizá el valor más significativo de ECySAP en el contexto multidominio radica en su contribución a la aceleración del ciclo OODA (Observar, Orientar, Decidir, Actuar). Al proporcionar una visión integrada del entorno operativo que trasciende las divisiones artificiales entre dominios, la plataforma permite a los comandantes identificar oportunidades y amenazas que pasarían desapercibidas bajo enfoques compartimentados tradicionales. Esta aceleración del proceso decisorio constituye una ventaja decisiva en escenarios caracterizados por la alta velocidad de los acontecimientos y la constante evolución de la situación táctica (Pulido, 2021).

3 Marco doctrinal y normativo

3.1 La doctrina en ciberdefensa

La evolución doctrinal de la OTAN en ciberdefensa refleja la transformación del panorama de amenazas global. Desde los primeros ciberataques contra Estonia en 2007, la Alianza ha desarrollado progresivamente un corpus doctrinal robusto, incorporando el ciberespacio como dimensión crítica de la seguridad euroatlántica. La Cumbre de Lisboa (2010) marcó el primer reconocimiento formal de las ciberamenazas en el Concepto Estratégico, pero fue la Cumbre de Varsovia (2016) la que consolidó el *Cyber Security Pledge*, comprometiendo a los aliados a fortalecer sus capacidades nacionales como contribución esencial a la Defensa Colectiva (Warsaw Summit Communiqué, OTAN, 2016).

La evolución continuó en la Cumbre de Bruselas (2018) con el establecimiento del Cyberspace Operations Centre (CyOC) en Mons y en Londres (2019) con la creación del NATO Cyber Security Centre (NCSC). Ambas estructuras operan bajo el NATO Communications and Information Agency (NCIA) y garantizan capacidades defensivas robustas y la protección de redes C3 críticas para el mando y control (Brussels Summit Declaration, OTAN, 2018). La Cumbre de Madrid (2022) profundizó este compromiso, estableciendo el Marco Estratégico Reforzado para la Ciberdefensa, que integra la disuasión, defensa y resiliencia cibernéticas en la postura general de la Alianza (Madrid Summit Declaration, OTAN, 2022).

El documento MC 0665 *NATO Military Concept for Cyberspace Operations* define el enfoque militar aliado para operaciones en el ciberespacio y

estableció tres funciones principales: protección de redes, operaciones defensivas y apoyo a operaciones cinéticas (NATO Military Concept for Cyberspace Operations, OTAN, 2018). Este concepto se desarrolla en la doctrina AJP-3.20, que proporciona directrices detalladas sobre planificación, ejecución y evaluación de operaciones cibernéticas, definiendo procesos para la integración del ciberespacio con operaciones terrestres, marítimas, aéreas y espaciales (Allied Joint Doctrine for Cyberspace Operations, OTAN, 2020).

Los ejercicios *Cyber Coalition* y *Locked Shields* han permitido a la OTAN probar y mejorar sus doctrinas, proporcionando escenarios realistas para validar conceptos operativos. El ejercicio *Crossed Swords* se centra, sobre todo, en técnicas ofensivas dentro del marco legal internacional, permitiendo el desarrollo de capacidades avanzadas para contrarrestar amenazas emergentes (CCDCOE Exercise Reports, OTAN, 2023).

La aplicación del artículo 5 al ámbito cibernético sigue un enfoque de umbral, donde la determinación de un «ataque armado» depende de la evaluación de escala, efectos, intencionalidad y atribución (Strategic Concept, OTAN, 2022). Esta aproximación, respaldada por el Manual de Tallin 2.0, proporciona flexibilidad estratégica mientras establece líneas rojas creíbles frente a adversarios potenciales (Schmitt, 2017).

ECYSAP implementa estos principios doctrinales mediante capacidades de fusión de inteligencia multifuente, análisis avanzado de amenazas y herramientas de respuesta coordinada, alineándose con el concepto OTAN de *Federated Mission Networking* para garantizar interoperabilidad y coherencia operativa en entornos multinacionales.

3.2 Marco normativo

El entramado normativo que sustenta la ciberseguridad europea constituye un ecosistema complejo y multinivel en constante evolución. La Directiva NIS2 (2022/2555) representa su piedra angular, ampliando considerablemente el alcance regulatorio a dieciocho sectores críticos e introduciendo un régimen de supervisión más estricto con sanciones de hasta 10 millones de euros o el 2 % de la facturación global anual. Establece mecanismos de notificación de incidentes en tres fases (24h/ 72h/ 1 mes) y exige medidas técnicas y organizativas proporcionadas al riesgo (La Directiva SRI2, Comisión Europea, 2023).

El Reglamento de Ciberresiliencia (2024/1313) complementa este marco abordando productos conectados, estableciendo requisitos de seguridad desde el diseño y obligaciones para fabricantes durante todo el ciclo de vida del producto. Su enfoque *Security by Design* representa un cambio paradigmático hacia la responsabilidad proactiva (Reglamento de Ciberresiliencia,

UE, 2024). Paralelamente, el Reglamento DORA (2022/2554) establece un régimen específico para el sector financiero, incluyendo pruebas de penetración avanzadas (TLPT) y gestión de riesgos de terceros proveedores críticos (TPRM), reconociendo la interconexión entre estabilidad financiera y ciberseguridad (Parlamento Europeo, 2022).

La Ley de Ciberseguridad (Cybersecurity Act, 2019/881) fortalece el mandato de ENISA y establece el marco europeo de certificación de ciberseguridad, creando esquemas sectoriales como EUCC para productos TIC y EUCS para servicios *cloud* (ENISA Certification Framework, 2023). La Directiva CER (2016/1148) aborda infraestructuras críticas, mientras que el Reglamento eIDAS2 (2023/2084) actualiza el marco de identidad digital, incorporando la *wallet* europea y reforzando los requisitos para servicios de confianza cualificados (eIDAS 2.0, Comisión Europea, 2023).

A nivel nacional, España transpuso la Directiva NIS2 mediante el Real Decreto-ley 3/2024, creando la Oficina Nacional de Ciberseguridad y reforzando las capacidades del CCN-CERT (BOE, 2024). Francia implementó la *Loi de Programmation Militaire* (2019-2025) con disposiciones específicas sobre ciberdefensa y capacidades ofensivas bajo el Commandement de la Cyberdéfense (COMCYBER) (Ministère des Armées, 2022). Alemania adoptó el IT-Sicherheitsgesetz 2.0, otorgando poderes ampliados al BSI para auditar infraestructuras críticas y establecer el *KRITIS-Dachgesetz* para estandarizar la protección sectorial (Germany - Federal Government, 2024). Italia desarrolló el *Perimetro di Sicurezza Nazionale Cibernetica* mediante el Decreto-Legge 105/2019, estableciendo la Agenzia per la Cybersicurezza Nazionale (ACN) como autoridad nacional (Gazzetta Ufficiale, 2021).

Los estándares ISO/IEC 27001:2022 (gestión de seguridad), ISO/IEC 27032:2023 (ciberseguridad), y ISO/IEC 42001:2023 (gobernanza de IA) proporcionan marcos técnicos globalmente reconocidos, mientras que el NIST Cybersecurity Framework 2.0 ofrece un enfoque complementario basado en funciones (identificar, proteger, detectar, responder, recuperar) ampliamente adoptado por organizaciones europeas (ISO/NIST Standards, 2023).

ECYSAP implementa este complejo entramado normativo mediante una arquitectura modular que garantiza el cumplimiento multinivel, incorporando capacidades específicas para la gestión del riesgo regulatorio y la adaptación ágil a requisitos emergentes. Su diseño facilita la interoperabilidad con estructuras nacionales de ciberseguridad y defensa, alineándose con los principios de soberanía digital europea mientras mantiene compatibilidad con estándares OTAN, ejemplificando la aproximación «Brussels-Washington» que caracteriza la ciberseguridad europea moderna (EU Cybersecurity Strategy, 2023).

4 Caso de uso

La anexión de Crimea por parte de Rusia en 2014 representó una operación multidominio compleja, donde las acciones en el ciberespacio jugaron un papel más que importante, como en el caso del ataque al sistema gubernamental ucraniano mediante el uso del arma cibernética «Ouroboros» o también llamada Snake, en marzo del año 2014 (Ross, 2014) o, según declaró la empresa CrowdStrike, el ataque con *malware* en el *software* utilizado en los Obús D-20 de Ucrania, lo que provocó la destrucción de un porcentaje elevado de los mismos (Zaks, 2017). A continuación, vamos a realizar un ejercicio de imaginación hipotético sobre cómo ECySAP podría haber sido utilizada para comprender, gestionar y mitigar los riesgos asociados a esta operación.

4.1 Contexto histórico: guerra mosaico y anexión de Crimea

En febrero de 2014, Rusia ocupó y, posteriormente, anexionó la península de Crimea, territorio de Ucrania. Esta operación constituyó un ejemplo paradigmático de guerra híbrida moderna, combinando operaciones militares convencionales con acciones cibernéticas, guerra de información y operaciones encubiertas. Como señala la evaluación oficial de la OTAN, «la anexión ilegal e ilegítima de Crimea» representó una flagrante violación del derecho internacional y un desafío directo al orden de seguridad europeo (Wales Summit Declaration, OTAN, 2022).

En el caso de Crimea, se observa cómo Rusia implementó una estrategia que combinó elementos discretos, pero coordinados: operaciones cibernéticas contra infraestructuras críticas, campañas de desinformación en medios tradicionales y redes sociales, despliegue de tropas sin insignias «hombres de verde» y acciones diplomáticas para legitimar la anexión. Esta combinación de elementos heterogéneos actuando en concierto ejemplifica los principios de la guerra mosaico, donde la sinergia entre componentes diversos crea efectos que superan la suma de sus partes individuales.

Según el Centro de Estudios Estratégicos e Internacionales (CSIS), la anexión de Crimea marcó el inicio de una nueva era en la conducción de operaciones cibernéticas como parte integral de campañas militares más amplias, estableciendo un patrón que se ha replicado y refinado en conflictos posteriores (CSIS, 2023). La Agencia de Ciberseguridad de Canadá ha documentado cómo, desde 2014, Ucrania ha tenido que mejorar significativamente sus capacidades de ciberdefensa en respuesta a las persistentes amenazas rusas (Cyber Centre Canada, 2022).

En este contexto, una plataforma como ECySAP resultaría especialmente valiosa, ya que proporcionaría la capacidad de integrar información proveniente de múltiples fuentes y dominios, generando una conciencia

situacional unificada que permita contrarrestar las estrategias de guerra mosaico. Al igual que el concepto de guerra mosaico enfatiza la flexibilidad y adaptabilidad de las operaciones militares, ECySAP está diseñada para adaptarse rápido a un panorama de amenazas constantes, proporcionando las herramientas necesarias para mantener la ventaja operativa en escenarios complejos.

4.2 Capas de Análisis de ECySAP en el contexto Crimea-Rusia

En este contexto, desde la perspectiva de ECySAP, el análisis comenzaría con una evaluación de las capas de misión y de sistemas de información y comunicación (CIS). Entre otros objetivos rusos, uno estratégico era asegurar el control de Crimea, protegiendo sus intereses geopolíticos y militares en la región, lo que incluía asegurar la base naval de Sebastopol y proyectar influencia en el mar Negro. Las tareas operativas incluían el despliegue de fuerzas, la realización del referéndum y la integración de Crimea en la Federación Rusa. Por otro lado, los servicios CIS críticos incluían telecomunicaciones, sistemas de información gubernamentales ucranianos, infraestructura de energía y redes de medios, cada uno sujeto a riesgos de ataques cibernéticos dirigidos a interrumpir las comunicaciones, difundir desinformación e influir en la opinión pública.

En el análisis de riesgos y evaluación de incidentes, ECySAP se centraría en la identificación de activos críticos, como servidores gubernamentales ucranianos en Crimea, la infraestructura de telecomunicaciones que conecta Crimea con Ucrania continental y los sistemas de control de la infraestructura energética en la península. Continuaría con una evaluación de riesgos y vulnerabilidades para analizar vulnerabilidades explotables y posibles campañas de desinformación. Un análisis de resiliencia cibernética evaluaría la capacidad de los sistemas ucranianos para resistir ataques y mantener la integridad de la información. Por último, se evaluaría el impacto en la misión proyectando vistas sobre cómo los ataques cibernéticos podrían afectar a una misión específica, la capacidad de Ucrania para responder a la intervención rusa y mantener el control sobre Crimea, así como el riesgo del impacto de la desinformación en la opinión pública y la legitimidad del referéndum.

Si bien, de momento, ECySAP no cuenta con IA integrada, se está desarrollando ECySAP EYE, con lo que, con una posible futura integración de IA, podría mejorar su eficacia en este escenario. Algoritmos de aprendizaje automático podrían analizar el tráfico de red en tiempo real para detectar patrones maliciosos asociados con la actividad rusa. Sistemas basados en IA podrían aplicar contramedidas automatizadas, como el bloqueo de direcciones IP maliciosas o el aislamiento de sistemas comprometidos. Además, la IA podría estudiar el comportamiento de los atacantes rusos y elaborar perfiles de ciberataques, identificando las Tácticas, Técnicas y

Procedimientos (TTP) utilizados, lo que facilitaría la anticipación y prevención de dichas posibles amenazas.

En el contexto de la guerra mosaico, ECySAP podría haber facilitado la coordinación y sincronización de acciones en diferentes dominios, permitiendo la generación efectiva de redes de efectos. Esto implicaría una conciencia situacional multidominio, integrando información de diversas fuentes para construir una imagen completa de la situación operativa. En cuanto a las operaciones sincronizadas, ECySAP establecería correlaciones entre eventos cibernéticos y sus potenciales manifestaciones en otros dominios, como la detección de actividades de reconocimiento en redes militares ucranianas que se correlacionen con movimientos de tropas rusas. La plataforma facilitaría la modelización de *kill chains* multidominio, donde acciones iniciales en el ciberespacio, como la inhabilitación de sistemas de defensa aérea mediante ataques a su infraestructura de red, facilitarían operaciones subsiguientes en el dominio físico como incursiones aéreas.

4.3 Protección frente a la desinformación

En el escenario real de 2014, Rusia desplegó una masiva campaña de desinformación que sentó las bases para su intervención militar. Los medios estatales rusos como RT y Sputnik difundieron narrativas falsas sobre supuestas amenazas a la población ruso-parlante de Crimea, mientras que operaciones encubiertas en redes sociales amplificaban estos mensajes. La doctrina OTAN reconoce la desinformación como un componente integral de las amenazas híbridas, definiéndola como «la difusión intencional de información falsa destinada a engañar y manipular» (NATO's approach to counter information threats, OTAN, 2025).

Si ECySAP hubiera estado operativo en 2014 habría proporcionado capacidades fundamentales para contrarrestar esta campaña de desinformación. La plataforma habría monitorizado en tiempo real los flujos de información, identificando patrones anómalos y narrativas falsas mediante análisis de *big data* y procesamiento de lenguaje natural avanzado. Esto se alinea con el requisito establecido en la Directiva NIS2 de «desarrollar capacidades de detección temprana de amenazas» (Unión Europea, 2022a).

ECySAP habría analizado la difusión de noticias falsas en medios sociales, detectando la creación repentina de miles de cuentas automatizadas (*bots*) antes de la intervención militar, un indicador temprano de una operación coordinada. La plataforma habría correlacionado estas actividades de desinformación con movimientos de tropas rusas, estableciendo patrones que indicaban una operación inminente, proporcionando así lo que la doctrina AJP-3.20 denomina «capacidad de proyección situacional» (Allied Joint Doctrine for Cyberspace Operations, OTAN, 2020).

Adicionalmente, ECySAP habría proporcionado evidencia verificable a autoridades ucranianas y organizaciones internacionales sobre la campaña coordinada rusa, facilitando la atribución de las acciones, un aspecto crítico según la doctrina OTAN para determinar respuestas apropiadas. La plataforma también habría generado contenidos contrastados para contrarrestar la desinformación, contribuyendo a lo que la Política de Ciberdefensa de la UE denomina «resiliencia cognitiva» frente a campañas de manipulación (Comisión Europea, 2022).

4.4 Protección de infraestructura crítica

Durante la crisis de Crimea, Ucrania experimentó numerosos ciberataques contra su infraestructura crítica, incluyendo ataques de denegación de servicio (DDoS) contra sitios web gubernamentales, interrupciones en comunicaciones de telefonía móvil, bloqueo de comunicaciones entre unidades militares y disrupciones en servicios esenciales. La protección de infraestructuras críticas constituye un pilar fundamental tanto de la doctrina OTAN como del marco regulatorio europeo, con la Directiva NIS2 designando dieciocho sectores críticos que requieren medidas reforzadas de ciberseguridad.

La implementación de ECySAP habría proporcionado capacidades significativas para la protección de estas infraestructuras. La plataforma habría detectado temprano los intentos de infiltración en redes críticas ucranianas mediante análisis de tráfico de red y detección de anomalías, cumpliendo con el requisito establecido en el artículo 21 de la Directiva NIS2 de implementar «medidas técnicas y organizativas adecuadas y proporcionadas para gestionar los riesgos para la seguridad de las redes y sistemas de información» (Unión Europea, 2022a).

ECySAP habría identificado vulnerabilidades en sistemas SCADA de infraestructura energética, anticipado ataques a redes de telecomunicaciones basándose en patrones observados y monitoreado continuamente redes eléctricas, suministro de agua y sistemas de transporte para detectar anomalías. Esto se alinea con lo que la doctrina AJP-3.20 denomina «protección de infraestructuras de información críticas» (Allied Joint Doctrine for Cyberspace Operations, OTAN, 2020).

Asimismo, de acuerdo con el concepto de «Common Operational Picture» (COP) establecido en la doctrina OTAN MC 0665, que destaca la importancia de una visión compartida del entorno operativo para lograr una acción eficaz, el sistema habría ofrecido a las autoridades una visión unificada del estado de las infraestructuras críticas. Esto habría facilitado la toma de decisiones coordinadas y la priorización eficiente de los recursos defensivos (NATO Military Concept for Cyberspace Operations, OTAN, 2018).

Ante incidentes confirmados, ECYSAP habría alertado automáticamente sobre sistemas comprometidos para que los analistas los aísleran con la mayor celeridad posible y así evitar la propagación de ataques. Además, se podrían haber establecido canales de comunicación alternativos entre instalaciones críticas ante la interrupción de los primarios, implementando así los principios de «segmentación de redes» y «redundancia de sistemas críticos» recomendados por la Agencia de la Unión Europea para la Ciberseguridad (ENISA, 2023).

4.5 Protección de activos físicos militares

En el escenario de Crimea, los denominados «hombres de verde», soldados rusos sin insignias, tomaron control de instalaciones militares estratégicas, mientras se producía un bloqueo naval de la flota ucraniana, interferencia con sistemas de comunicación militar y deshabilitación de radares y sistemas de defensa aérea. La doctrina OTAN AJP-3.20 reconoce y subraya la creciente interconexión entre los dominios cibernético y físico, afirmando que «las operaciones en el ciberespacio pueden tener efectos cinéticos» (Allied Joint Doctrine for Cyberspace Operations, OTAN, 2020).

ECySAP habría proporcionado capacidades para la protección de activos militares en este escenario. La plataforma habría alertado sobre interferencias electromagnéticas en sistemas de navegación y comunicación militar mediante análisis del espectro electromagnético y correlación con actividades cibernéticas. Habría detectado patrones anómalos de comunicaciones en las cercanías de bases militares ucranianas, proporcionando alertas tempranas de actividades hostiles inminentes.

Un aspecto en particular relevante habría sido la capacidad de ECySAP para identificar la suplantación de señales GPS utilizadas para confundir a unidades ucranianas, una técnica de guerra electrónica empleada por Rusia durante el conflicto. La doctrina OTAN MC 0665 identifica la guerra electrónica como un componente crítico de las operaciones híbridas modernas, estrechamente vinculado a las capacidades cibernéticas (NATO Military Concept for Cyberspace Operations, OTAN, 2018).

La plataforma habría correlacionado eventos cibernéticos con actividades físicas sospechosas alrededor de activos militares, proporcionando un análisis multidominio «Multi-Domain Operations» (Allied Joint Doctrine, OTAN, 2021) que habría facilitado la comprensión holística de la situación.

Además, ECySAP habría proporcionado información necesaria al comandante para valorar rutas seguras para la evacuación o refuerzo de instalaciones críticas, mantenido comunicaciones seguras entre el mando central ucraniano y las unidades desplegadas en Crimea y permitido la operación remota de sistemas defensivos aun después de la ocupación física

de instalaciones. Estas capacidades implementan el principio de «resiliencia operativa» establecido en la Directiva NIS2, que requiere «medidas para asegurar la continuidad de servicios críticos incluso bajo condiciones adversas» (Unión Europea, 2022a).

4.6 Conclusiones caso de uso

El uso hipotético de ECySAP en la anexión de Crimea demuestra cómo una plataforma integral de conciencia situacional cibernética podría ser utilizada para comprender, gestionar y mitigar los riesgos asociados a operaciones multidominio complejas. ECySAP, en este caso, podría haber proporcionado una información valiosa para la toma de decisiones y la planificación de respuestas.

Adicionalmente, aunque se destaca y se recuerda que este planteamiento es meramente un enfoque hipotético basado en las capacidades potenciales de ECySAP, la experiencia de Crimea podría evidenciar cinco características fundamentales de los conflictos contemporáneos que ECySAP sería capaz de abordar:

- La línea entre paz y guerra se difumina en escenarios de conflicto híbrido, creando lo que la doctrina OTAN denomina «zona gris» donde se desarrollan actividades hostiles sin llegar a un conflicto armado declarado (Allied Joint Doctrine, OTAN, 2021). ECySAP proporcionaría herramientas necesarias para detectar y responder a amenazas en este espectro ambiguo.
- En un ambiente bélico, los ataques comienzan en el ciberespacio antes de manifestarse físicamente, siguiendo lo que el Centro de Excelencia de Ciberdefensa Cooperativa de la OTAN (CCDCOE) denomina «modelo de operaciones cibernéticas preparatorias» (CCDCOE, 2023). ECySAP permitiría la detección temprana de estas actividades preparatorias, facilitando respuestas preventivas.
- El sistema ECySAP proporcionaría capacidades para detectar y contrarrestar campañas de desinformación. Esta última prepara el terreno para operaciones militares convencionales, como parte de lo que la doctrina OTAN MC 0665 identifica como «operaciones de información» destinadas a «influir en las percepciones, actitudes y comportamientos» (NATO Military Concept for Cyberspace Operations, OTAN, 2018).
- La Directiva NIS2 reconoce que la integridad de infraestructuras críticas se convierte en objetivo prioritario, y es importante establecer medidas reforzadas para su protección (Unión Europea, 2022a). ECySAP podría proporcionar un marco integrado para la protección de esta tipología de infraestructuras.

5 Conclusiones

En un entorno internacional caracterizado por la competición estratégica y el protagonismo creciente de las operaciones en el ciberespacio, el desarrollo de capacidades avanzadas de Conciencia Situacional Cibernética constituye ya no una ventaja opcional sino un requisito indispensable para la seguridad nacional. Las organizaciones militares y de seguridad que no logren adaptarse a este nuevo paradigma se encontrarán en desventaja significativa frente a adversarios tecnológicamente avanzados.

El futuro desarrollo de la CySA deberá afrontar distintos desafíos, especialmente, en lo relativo a la integración de fuentes heterogéneas de datos, la traducción de indicadores técnicos en implicaciones operativas y la evaluación objetiva de su impacto real. La colaboración entre el ámbito académico, la industria y las organizaciones de defensa resultará crucial para superar estas limitaciones y maximizar el potencial de herramientas como ECySAP.

En última instancia, el valor estratégico de la Conciencia Situacional Cibernética radica en su capacidad para reducir la incertidumbre y acelerar el ciclo OODA en entornos complejos y dinámicos. En un mundo donde la superioridad informativa constituye un factor determinante del éxito operativo, la inversión en estas capacidades representa una prioridad ineludible para cualquier nación que aspire a garantizar su seguridad en el complejo escenario geopolítico del siglo XXI.

Bibliografía

Agencia de la Unión Europea para la Ciberseguridad (ENISA). (2023). *Recomendaciones para la segmentación de redes y sistemas críticos*. Heraklion, ENISA.

Alianza Atlántica. (2022). *Marco estratégico para la ciberdefensa en el ámbito de la OTAN*. Bruselas, OTAN.

Barford, P., Dacier, M., Dietterich, T., Fredrikson, M., Giffin, J., Jajodia, S., y Ou, X. (2010). Cyber Situational Awareness: Issues and Research. *Advances in Information Security*. 46, pp. 3-13.

Boyd, J. (1976). *Destruction and Creation*. U.S. Army Command and General Staff College.

Centro de Estudios Estratégicos e Internacionales (CSIS). (2023). *Cyber Operations during the Russo-Ukrainian War*. Washington, CSIS.

Centro de Excelencia de Ciberdefensa Cooperativa de la OTAN (CCDCOE). (2023). *Estrategias de operaciones cibernéticas en conflictos modernos*. Tallin, CCDCOE.

Chatzimichailidou, M. M., Protopapas, A., & Dokas, I. M. (2015). Seven issues on distributed situation awareness measurement in complex socio-technical systems. In F. Boulanger, D. Krob, G. Morel, & J.-C. Roussel (Eds.), Complex systems design & management (pp. 89–101). Springer. https://doi.org/10.1007/978-3-319-11617-4_8

Comisión Europea. (2022). *Política de Ciberdefensa de la UE*. COM (2022) 49 final. Bruselas, Comisión Europea.

Comisión Europea. (2023). *La Directiva SRI2: asegurar las redes y los sistemas de información*. Bruselas: Comisión Europea.

Comunicación Oficial Demostrador. (2025). Informe ECySAP: Evaluación de impacto cibernético en operaciones. Documento interno de proyecto.

Cyber Centre Canada. (2022). *Cyber threat bulletin: Cyber threat activity related to the Russian invasion of Ukraine*. Ottawa, Communications Security Establishment.

Endsley, M. R. (1988). Design and evaluation for situation awareness enhancement. *Proceedings of the Human Factors Society Annual Meeting*. 32(2), pp. 97-101.

Endsley, M. R., y Connors, E. (2008). Situation awareness: State of the art. *2008 IEEE Power and Energy Society General Meeting – Conversion and Delivery of Electrical Energy in the 21st Century*. Pittsburgh, pp. 1-4.

Esteve, M., Pérez, I., Palau, C., Carvajal, F., Hingant, J., Fresneda, M. A., & Sierra, J. P. (2016). Cyber Common Operational Picture: A Tool for Cyber Hybrid Situational Awareness Improvement. North Atlantic Treaty Organization (NATO) Science and Technology Organization (STO), Technical Report STO-MP-IST-148.

Fojon, E. (2020). Nuevos paradigmas militares en la era de la Competición Estratégica: el caso de las operaciones anfibias y la guerra mosaico. Real Instituto Elcano, ARI 13/2020.

Franke, U. y Brynielsson, J. (2014). Cyber situational awareness: A systematic review of the literature. *Computers & Security*. 46, pp. 18-31.

Gazzetta Ufficiale. (2021). Decreto-legge 14 giugno 2021, n. 82, convertido en Legge 4 agosto 2021, n. 109: creación de la Agenzia per la Cybersicurezza Nazionale (ACN). https://www.gazzettaufficiale.it/eli/id/2021/06/14/21G00098/SG; https://www.gazzettaufficiale.it/eli/id/2021/08/04/21A04841/sg

Germany – Federal Government. (2024). Draft KRITIS-Dachgesetz (Ley marco de infraestructura crítica) – Comunicado y documentación.

(Resumen oficial del proceso legislativo 2024). https://www.bmi.bund.de

Indra. (2021). ECySAP: Enhanced Cyber Situational Awareness Platform. *Technical White Paper*.

Indra, Unidad de Ciberdefensa. (2024). *Documento interno*. (Documento no publicado).

Jajodia, S., Liu, P., Swarup, V., & Wang, C. (2010). Cyber situational awareness: Issues and research. In S. Jajodia, P. Liu, V. Swarup, & C. Wang (Eds.), *Cyber Situational Awareness: Issues and Research* (pp. iii-iv). (Advances in Information Security; Vol. 46). https://doi.org/10.1007/978-1-4419-0140-8

Jordán, J. (2023). Guerra mosaico: qué es y a qué desafíos se enfrenta. Revista de Aeronáutica y Astronáutica, (920), 160-167.

Kim, J., Jeong, S., Kim, J., & Lee, J. (2022). Study on cyberattack damage assessment framework. IEEE Access, 10, 59270–59276. https://doi.org/10.1109/ACCESS.2022.3179977

Kim, K., Youn, J., Yoon, S., Kang, J., Kim, K., & Shin, D. (2023). Study on Cyber Common Operational Picture framework for cyber situational awareness. Applied Sciences, 13(4), 2331. https://doi.org/10.3390/app13042331

Llopis Sánchez, S. (2023). Decision support elements and enabling techniques to achieve a cyber defence situational awareness capability (Doctoral dissertation, Universitat Politècnica de València).

Llopis Sanchez, S., & Lopes Antunes, D. (2024). Operation assessment in cyberspace: Understanding the effects of cyber deception. Proceedings of the 19th International Conference on Availability, Reliability and Security (pp. 1-8). Association for Computing Machinery. https://doi.org/10.1145/3664476.3672355

Llopis, S., Hingant, J., Pérez, I., Esteve, M., Carvajal, F., Mees, W., & Debatty, T. (2018). A comparative analysis of visualisation techniques to achieve cyber situational awareness in the military. In 2018 International Conference on Military Communications and Information Systems (ICMCIS) (pp. 1-7). IEEE.

López Díaz, J. A. (2020). Guerra Mosaico vs Confrontación de Sistemas. Cuaderno de Pensamiento Naval, Número 28, 49-68.

Maestre Vidal, J., Sotelo Monge, M. A., Rodríguez López, F. A., Mateos Calle, M., Estevez Tapiador, J. M., Villagrá González, V., Tornero Sánchez, D., Gómez Henche, R., & Aragonés Lozano, M. (2022). Plataforma Europea para adquisición de Consciencia de Situación

del Ciberespacio. En Actas de las VIII Jornadas Nacionales de Investigación en Ciberseguridad (JNIC 2022) (Vol. 11, pp. xx–xx). Red de Excelencia Nacional de Investigación en Ciberseguridad. https://2022.jnic.es/Actas_JNIC_2022_v11.pdf

McGuinness, B., & Foy, L. (2000). A Subjective Measure of SA: The Crew Awareness Rating Scale (CARS). In Human performance, situation awareness and automation conference; user-centered design for the new millennium (pp. 286-291). SA Technologies.

Ministère des Armées. (2022). Commandement de la cyberdéfense (COMCYBER) – misión y organización (página oficial). https://www.defense.gouv.fr/comcyber

Ministerio para la Transformación Digital y de la Función Pública. (2024, 30 de abril). Real Decreto 443/2024, de 30 de abril, por el que se aprueba el Esquema Nacional de Seguridad de redes y servicios 5G (BOE núm. 106, pp. 49754–49801). Boletín Oficial del Estado. https://www.boe.es/buscar/act.php?id=BOE-A-2024-8715

NATO. (2018). NATO Military Concept for Cyberspace Operations (MCCO). https://www.nato.int/cps/en/natohq/

NATO. (2021). AJP-3.20 Allied Joint Doctrine for Cyberspace Operations (Edition A, Version 1). (Edición abierta reproducida) https://iwar.org.uk/wp-content/uploads/2021/06/AJP-3.20-EDA-V1-E.pdf

NATO Allied Command Operations. (2010). Comprehensive Operations Planning Directive (COPD). Norfolk: ACO.

NATO Standardization Office. (2020). *AJP-3.20: Allied Joint Doctrine for Cyberspace Operations* (Edition A, Version 1). North Atlantic Treaty Organization. https://assets.publishing.service.gov.uk/media/5f086ec4d3bf7f2bef137675/doctrine_nato_cyberspace_operations_ajp_3_20_1_.pdf

NATO Standardization Office. (2024, abril). AJP-6 (Edition B, Version 1) – Allied Joint Doctrine for Communication and Information Systems. NATO. https://www.coemed.org/files/stanags/01_AJP/AJP-6_EDB_V1_E_2525.pdf

North Atlantic Treaty Organization. (2016, July 9). Warsaw Summit Communiqué. https://www.nato.int/cps/en/natohq/official_texts_133169.htm

North Atlantic Treaty Organization. (2019, July 11). Brussels Summit Declaration. https://www.nato.int/cps/fr/natohq/official_texts_156624.htm

North Atlantic Treaty Organization. (2022, June 29). Madrid Summit Declaration. https://www.nato.int/cps/en/natohq/official_texts_196951.htm

Onwubiko, C. (2016). Understanding cyber situation awareness. International Journal on Cyber Situational Awareness, 1(1), 11–30. https://doi.org/10.22619/IJCSA.2016.100101

OTAN. (2016-2025). *Cyber defence, doctrinas y conceptos militares en ciberseguridad*. Varsovia, Bruselas y Gales, OTAN.

Pulido, G. (2021). Guerra multidominio y mosaico: El nuevo pensamiento militar estadounidense. Los libros de la Catarata.

Real Instituto Elcano. (2020). *Nuevos paradigmas militares en la era de la Competición Estratégica: el caso de las operaciones anfibias y la guerra mosaico*. Madrid, Real Instituto Elcano.

Reglamento (UE) 2024/2847 del Parlamento Europeo y del Consejo. (2024, 23 de octubre). Reglamento sobre requisitos horizontales de ciberseguridad para productos con elementos digitales (Cyber Resilience Act). Diario Oficial de la Unión Europea, L 2847, 20 de noviembre de 2024. https://eur-lex.europa.eu/eli/reg/2024/2847/oj

Ross, A. (2014) Russia's cyber weapons hit Ukraine: How to declare war without declaring war. *The Christian Science Monitor*. [Consulta: 2025]. Disponible en: https://www.csmonitor.com/Commentary/Global-Viewpoint/2014/0312/Russia-s-cyber-weapons-hit-Ukraine-How-to-declare-war-without-declaring-war

Schaberreiter, T., Röning, J., Quirchmayr, G., et al. (2022). A cybersecurity situational awareness and information-sharing solution for local public administrations: The CS-AWARE project. En Challenges in Cybersecurity and Privacy – the European Research Landscape. CRC Press. https://doi.org/10.1201/9781003337492-8

Schmitt, M. N. (ed.). (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge, Cambridge University Press.

Tadda, G. P., & Salerno, J. S. (2010). Overview of cyber situation awareness. En S. Jajodia, P. Liu, V. Swarup, & C. Wang (Eds.), Cyber Situational Awareness: Issues and Research (Advances in Information Security, Vol. 46). Springer. https://doi.org/10.1007/978-1-4419-0140-8_2

Unión Europea. (2022a). Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE)

n.º 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (Directiva SRI 2). *Diario Oficial de la Unión Europea*. 27 de diciembre, L333.

Unión Europea. (2022b). Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 sobre la resiliencia operativa digital del sector financiero y por el que se modifican los Reglamentos (CE) n.º 1060/2009, (UE) n.º 648/2012. (UE) n.º 600/2014, (UE) n.º 909/2014 y (UE) 2016/1011. *Diario Oficial de la Unión Europea*. 27 de diciembre, L333.

U.S. Army (2023). ATP 3-12.3, Electromagnetic Warfare Techniques. https://irp.fas.org/doddir/army/atp3-12-3.pdf

U.S. Department of the Army. (2021). *Field Manual 3-12: Cyberspace and electronic warfare operations (FM 3-12)*. Headquarters, Department of the Army. https://irp.fas.org/doddir/army/fm3-12.pdf

Zaks, D. (2017). Ukraine's military denies Russian hack attack. *RFI*. [Consulta: 2025]. Disponible en: https://www.rfi.fr/en/contenu/20170106-ukraines-military-denies-russian-hack-attack