La innovación tecnológica en el área de la inteligencia de ciberamenazas y por extensión de la ciberdefensa

Juan Adolfo Montero

Resumen

La ciberseguridad tradicional se enfoca en proteger sistemas de amenazas genéricas, siendo insuficiente frente a actores estatales avanzados con intenciones militares específicas. Para abordar este desafío, surge la ciberdefensa, que integra la inteligencia de ciberamenazas para planificar y conducir operaciones defensivas adaptadas a amenazas concretas.

La ciberdefensa se basa en tres pilares:

- La Misión: garantiza que los sistemas críticos estén protegidos para el éxito operativo.
- La Amenaza: evalúa adversarios, tácticas y herramientas empleadas.
- El Ciberespacio: identifica vulnerabilidades, rutas de ataque y zonas estratégicas para establecer defensas efectivas.

Para mejorar la eficacia defensiva, se han desarrollado tecnologías avanzadas como PICO, una plataforma que integra inteligencia de ciberamenazas y la Gestión de Incidentes y ECySAP, que evolucionará desde un Sistema de Cyber Situational Awarenes hacia un sistema de mando y control de ciberoperaciones.

Además, ambos proyectos (junto a alguno más también en desarrollo) se integrarán en el programa SCOMCE, el cual aplicará tecnologías como Datalakes, inteligencia artificial y simulación para detectar patrones, predecir ataques y automatizar respuestas.

El éxito de la Ciberdefensa dependerá no solo de estas herramientas, sino también de personal altamente capacitado y de una industria tecnológica nacional que garantice independencia estratégica en la protección del ciberespacio militar.

Palabras clave

Ciberdefensa, Ciberespacio, PICO, ECYSAP, SCOMCE.

Technological innovation in the area of cyber threat intelligence and, by extension, cyber defense

Abstract

Traditional Cybersecurity focuses on protecting systems from generic threats, which is insufficient against advanced state actors with specific military intentions. To address this challenge, Cyber Defense has emerged, integrating Cyber Threat Intelligence to plan and conduct defensive operations tailored to specific threats.

Cyber Defense is based on three pillars:

The Mission: Ensures Critical Systems to be protected to guarantee operational success.

The Threat: Assesses adversaries, tactics, techniques, procedures and tools employed.

The Cyberspace: Identifies vulnerabilities, attack routes, and strategic zones to establish effective defenses.

To enhance defensive effectiveness and capabilities MCCE have acquired advanced technologies such as the PICO Platform, that integrates Threat Intelligence and Incident Management capabilities, and will acquire a CYSA capability based on ECYSAP project, which will evolve from a Cyber Situational Awareness System to a Cyber Defense Command and Control System.

Both projects, together with some others already developed for MCCE, will be integrated in the Spanish SCOMCE program. The SCOMCE program will apply technologies like Datalakes, Artificial Intelligence, and Simulation to detect patterns, predict attacks, and automate responses.

The success of Cyber Defense will depend not only on these tools but also on highly trained personnel and a national technology industry that ensures strategic independence in the defence of military Cyberspace.

Keywords

Cyberdefence, Cyberspace, PICO, ECYSAP, SCOMCE.

1 Introducción: la inteligencia de ciberamenazas como base de la transición de la ciberseguridad a la ciberdefensa

Durante años, la ciberseguridad ha sido el eje central del desarrollo tecnológico en materia de protección del ciberespacio[1]. La investigación, desarrollo e innovación (I+D+i) han estado orientados a generar productos destinados, principalmente, al ámbito civil, con el objetivo de hacer frente a amenazas generales y no dirigidas. Este enfoque, lógico dentro de contextos empresariales o institucionales, se centra en la protección básica de sistemas[2] y servicios frente a riesgos comunes en el ciberespacio. (Seguritecnia, 2023)

Sin embargo, al analizar estos mismos productos desde una óptica militar, se revela una carencia importante: no contemplan aspectos tácticos, operacionales ni estratégicos propios de las operaciones militares. Tampoco están diseñados para enfrentarse a amenazas específicas y sofisticadas que afectan directamente a la Defensa Nacional ni responden a las prioridades operativas derivadas de las misiones en curso.

Durante mucho tiempo, las Fuerzas Armadas adoptaron herramientas comerciales de ciberseguridad, aplicándolas en contextos militares con un enfoque similar al civil. No obstante, la realidad del ciberespacio como nuevo dominio de las operaciones ha demostrado que este enfoque resulta insuficiente. Se hace indispensable integrar un modelo más amplio: la ciberdefensa, que complemente la ciberseguridad con un análisis orientado a las necesidades específicas del entorno militar.

En este contexto de ciberespacio de interés militar, los sistemas de ciberseguridad convencionales no son un obstáculo real frente a actores estatales con grandes capacidades y recursos (tecnológicos, económicos y humanos) y con objetivos estratégicos (geopolíticos y militares) claros. Estos adversarios pueden emplear herramientas especializadas para evadir fácilmente los mecanismos tradicionales de protección (ciberseguridad). (Real Instituto Elcano, s. f.)

---

[1] En este artículo nos referiremos como ciberespacio (o a veces, como «sistemas» en general), a cualquier sistema CIS, plataformas o sistema de combate, o sistema de armas que entre sus componentes se encuentra elementos de ***software*** dentro del mismo, así como infraestructuras y servicios civiles dependientes de tecnología IT/OT y que sean soporte de las capacidades militares o de los poderes del Estado y sean, por tanto, críticos para la Defensa y Seguridad Nacional.

[2] Bajo el término «Sistema» nos referiremos en este artículo a cualquier Sistema CIS, plataformas/sistema de combate o sistema de armas que, entre sus componentes, se encuentran elementos de ***software*** dentro del mismo, así como infraestructuras y servicios civiles dependientes de tecnología IT/OT y que sean soporte de las capacidades militares o de los poderes del Estado y sean, por tanto, críticos para la Defensa y Seguridad Nacional.

1.1 ¿Por qué la ciberseguridad tradicional ya no es suficiente? (Rodríguez, 2023)

— Porque los adversarios emplean tecnologías avanzadas capaces de eludir los sistemas convencionales de ciberseguridad.

— Porque las soluciones comerciales están diseñadas y configuradas[3] para identificar amenazas comunes y no están optimizadas para detectar ni neutralizar amenazas específicas dirigidas a las Fuerzas Armadas.

Por esta razón, la ciberdefensa basada en Inteligencia de Ciberamenazas se posiciona como un elemento clave. Este enfoque permite:

— Obtener conciencia situacional del ciberespacio (CySA).

— Apoyar la toma de decisiones tácticas y operacionales y el planeamiento defensivo del ciberespacio con una perspectiva militar.

— Reconfigurar sistemas de ciberseguridad y ciberdefensa para responder de forma concreta a las amenazas específicas[4] que afectan directamente a la misión o a los intereses estratégicos.

Este tipo de inteligencia requiere una Plataforma de Inteligencia de Ciberamenazas (TIP[5]) especializada, capaz de adaptarse a las características únicas del entorno de las operaciones en el ciberespacio de interés militar.

La creciente actividad de servicios secretos, unidades militares de operaciones en el ciberespacio o grupos intermediarios (*proxies*) subvencionados y apoyados por estados y naciones hostiles llevó a que, en 2016, durante la Cumbre de Varsovia, la OTAN reconociera el ciberespacio como un nuevo dominio o ámbito de las operaciones militares. Esta declaración supuso un giro conceptual: de una ciberseguridad reactiva y genérica (necesaria, pero insuficiente), hacia una ciberdefensa basada en la planificación y la inteligencia de ciberamenazas. (NATO, 2016)

---

[3] Los sistemas de ciberseguridad están diseñados y configurados con reglas de detección para detectar los modus operandi más habituales y comunes a la generalidad de las amenazas, pero no está especializada, ni prioriza la capacidad de detección/reacción frente a actores de la ciberamenazas específica a la que las FAS deben de hacer frente. La ciberseguridad comercial se basa en detectar indicadores técnicos de compromiso (IOC) o comportamientos anómalos, pero no ofrece una defensa táctica o estratégica ante adversarios con intenciones claras y persistentes contra intereses nacionales o de la Defensa y Seguridad Nacional.

[4] En función de la misión, de la coyuntura geopolítica, de la región o área de operaciones, etc.

[5] TIP son las siglas que se corresponden con: «Threat Intelligence Platform»

1.2 Diferencias clave entre ciberseguridad y ciberdefensa

La ciberdefensa no es solo una evolución de la ciberseguridad, sino un enfoque distinto que incorpora tres factores críticos:

1. La misión. ¿Qué funciones, capacidades, sistemas o servicio debemos proteger?
2. La amenaza específica. ¿Quién nos ataca o puede atacar?, ¿cómo y con qué intenciones?
3. Las debilidades del sistema. ¿Dónde somos vulnerables? ¿Dónde nos pueden atacar e impactarnos operativamente?

Desde esta óptica, el análisis de amenazas se convierte en un factor determinante. La ciberdefensa implica la planificación y conducción de una defensa predictiva y proactiva dirigida por inteligencia de ciberamenazas.

1.3 Analogía militar: ciberseguridad como defensa básica

Se puede comparar la «ciberseguridad tradicional» con los elementos básicos de «protección inmediata»[6] de una posición de infantería: alambradas, campos de minas, posiciones fijas. Son necesarios, sí, pero no suficientes para detener a un enemigo determinado, bien armado y con objetivos concretos. Estos mecanismos actúan como una protección inmediata, pero sin una visión táctica o estratégica.

La ciberdefensa, en cambio, se basa en inteligencia de ciberamenazas, planeamiento y adaptación, con el propósito de proteger el entorno del ciberespacio de interés militar en función de la misión militar, anticipando y neutralizando los movimientos del adversario.

2 La «Operacionalización» del ciberespacio

El concepto de «Operacionalización» del ciberespacio representa un cambio profundo en la forma de entender las operaciones en el ciberespacio. Hasta hace poco, las acciones en el ciberespacio se abordaban desde un enfoque puramente técnico. Sin embargo, este dominio ha comenzado a integrarse plenamente en el planeamiento y ejecución de las operaciones militares, aplicando principios tácticos y operacionales similares a los de otros ámbitos tradicionales de las operaciones militares (tierra, mar, aire, espacio). (Junta Interamericana de Defensa, 2023).

Este nuevo enfoque implica que las acciones defensivas en el ciberespacio ya no se basan únicamente en proteger sistemas de forma generalizada,

[6] Sin finalidad táctica, con la sola finalidad de dar cierta protección a los combatientes.

sino que ahora deben considerarse y analizarse en detalle tres factores clave:

— La amenaza concreta a enfrentar.
— La misión que se debe cumplir.
— Las vulnerabilidades del ciberespacio de interés militar a defender.

Gracias a esta evolución, comienzan a desarrollarse herramientas y tecnologías diseñadas específicamente con una mentalidad militar operativa, superando las limitaciones de los enfoques meramente técnicos. La atención ya no se centra en amenazas genéricas, sino en actores concretos, cuyas capacidades, motivaciones e intenciones se analizan a la luz de su contexto geopolítico, su área de influencia y sus objetivos estratégicos.

Esta transformación ha dado lugar a un tipo de inteligencia de ciberamenazas mucho más especializada, capaz de integrar en su análisis aspectos como:

— La región donde se desarrollan las operaciones.
— Las intenciones de los actores hostiles.
— Los intereses militares y políticos que motivan posibles ataques.

En consecuencia, la operacionalizacion del ciberespacio no solo cambia el enfoque, sino que también incorpora el análisis de la ciberamenaza como un componente esencial para diseñar y ejecutar una defensa eficaz. Esta inclusión convierte a la ciberdefensa en un ámbito de operaciones que ya no puede limitarse a prevenir o reaccionar ante incidentes, sino que debe anticiparse a ellos, basándose en una comprensión profunda del adversario, del entorno operativo y del ciberespacio militar sobre el que las operaciones descansan.

3 La ciberdefensa: un enfoque integral y dirigido por la Inteligencia de Ciberamenazas

Uno de los mayores desafíos en el ciberespacio es la clara ventaja con la que cuenta el atacante. Este puede decidir qué atacar, cuándo y cómo, utilizando técnicas, herramientas y *malware* a su antojo, y con el tiempo del mundo necesario para planificar y ejecutar su ofensiva. Por el contrario, el defensor debe proteger todo el sistema en su conjunto, sin saber con exactitud por dónde se producirá el ataque ni cuándo ni cómo.

3.1 Ventajas y desventajas del atacante y del defensor

El atacante solo necesita explotar una vulnerabilidad. El defensor, en cambio, debe asegurar todas. Esta asimetría define el carácter de la defensa del ciberespacio de interés militar: reactiva en su forma más básica, pero

con el potencial de ser proactiva y predictiva si se apoya en inteligencia especializada de ciberamenazas.

Aun así, el defensor dispone de ciertos recursos a su favor:

- Conocimiento del entorno a proteger (ciberterreno).
- Acceso a inteligencia de ciberamenazas, con un análisis histórico del comportamiento enemigo.
- Capacidad de modificar el ciberespacio de interés militar, aplicando configuraciones defensivas, reorganizaciones y contramedidas adaptadas.

3.2 Ciberdefensa: de la reacción a la anticipación

Frente a amenazas avanzadas como los APT[7] (Amenazas Persistentes Avanzadas), la ciberdefensa debe buscar anticipación, planificación, y actitud proactiva. Esto se logra mediante un enfoque que parta del análisis detallado de tres factores fundamentales:

3.2.1 La Amenaza

Implica identificar y comprender a los adversarios potenciales[8]:

— Sus capacidades y recursos.
— Sus motivaciones, intenciones y objetivos.
— Sus tácticas, técnicas y procedimientos (TTPs, *modus operandi*).
— Herramientas, *malware*, vulnerabilidades que explotan, etc.

Este conocimiento permite planificar operaciones defensivas dirigidas por inteligencia específica de ciberamenazas *(Intel-Driven Defensive Cyber Operations*).

3.2.2 La Misión

La defensa no puede ser genérica. Debe enfocarse en proteger los sistemas y servicios críticos para el éxito de la operación militar. Este enfoque se enmarca en el concepto de Mission Assurance. Para ello se analiza:

— ¿Qué partes del ciberespacio[9] son esenciales o críticas para la misión?

[7] APT son siglas que se corresponden con: «Advanced Persistent Threat». Es decir, actores de la amenaza con grandes recursos humanos, económicos, tecnológicos y procedimentales. Normalmente subvencionados y apoyados por Estados y con intereses geopolíticos, estratégico-políticos, y militares.
[8] Por lo general, APT compuestos por unidades militares de operaciones en el ciberespacio estatales o servicios secretos y grupos criminales (Proxies) apoyadas y subvencionadas por estados hostiles.
[9] Elementos o servicios críticos del ciberespacio que debemos, prioritariamente, defender para alcanzar el objetivo de Mission Assurance.

— ¿Qué sistemas, si son atacados, pueden, potencialmente, impactar más negativamente en la misión?
— ¿Cuál sería el impacto potencial si fueran atacados?
— ¿Qué servicios y activos son prioritarios entonces que defendamos?

El análisis de nuestro «Centro de Gravedad» operacional, de las capacidades críticas, de las dependencias de esas capacidades respecto a zonas del ciberespacio de interés militar, y de las vulnerabilidades que presentan estas zonas[10], ayuda a identificar los objetivos potenciales del adversario y las áreas prioritarias a defender.

3.2.3 El ciberespacio a defender[11]

Una vez definidos los activos y servicios clave[12], se debe analizar:

— Sus vulnerabilidades[13] técnicas y tácticas.
— Las posibles avenidas de aproximación del adversario[14]: rutas que podría utilizar para infiltrarse, avanzar y alcanzar sus objetivos.
— Las zonas vulnerables o menos protegidas del ciberespacio a defender.

Aquí, la inteligencia avanzada de la ciberamenaza es la clave para pasar de una defensa reactiva a una preventiva y planificada.

3.3 Aplicación de inteligencia táctica, operacional y estratégica

Para planificar y ejecutar la defensa, se requiere aplicar inteligencia de ciberamenazas en todos los niveles:

— Táctica: analiza vulnerabilidades defensivas, servicios críticos, posibles rutas de acceso del enemigo, intenciones y capacidades. Permite definir el plan defensivo de nivel táctico.
— Operacional: estudia las acciones y efectos que el adversario puede buscar para alcanzar sus objetivos más amplios (operacionales y estratégicos).

---

[10] Estas zonas del ciberespacio estarán formadas por servicios, sistemas, plataformas, etc.
[11] Esto incluye activos digitales, como bases de datos, aplicaciones críticas y sistemas operativos, así como infraestructura clave e información y datos críticos para la misión.
[12] Zonas prioritarias del ciberespacio a defender por interés militar.
[13] Tales como configuraciones inseguras, software desactualizado, interconexiones y puntos de vulnerabilidades del ciberespacio a defender que puedan ser explotados por el adversario en su ataque.
[14] Haciendo un símil al ámbito terrestre, se trataría Identificar los potenciales valles y vaguadas en el ciberespacio que podrían ser potencialmente empleado por el adversario como avenidas de aproximación, avance o ataque a sus objetivos. Estos valles o vaguadas en el ciberespacio estarían formados por las rutas formadas por los dispositivos y servicios más vulnerables y configurados de manera más insegura.

Estratégica: identifica actores clave[15] de la ciberamenaza, sus relaciones, capacidades estructurales, recursos tecnológicos y de formación y vínculos con gobiernos hostiles. Permitirá un planeamiento defensivo de nivel estratégico enfocado a atacar[16] las raíces de las capacidades ofensivas del adversario en el ciberespacio.

3.4 El modelo IPB aplicado al ciberespacio (Cyber-IPB)

Este enfoque, tomado del ámbito terrestre, se adapta a la ciberdefensa aplicando elementos y conceptos tácticos terrestres al ciberespacio.

El Cy-IPB es el resultado de un análisis cruzado (correlación) de los datos y la información disponible sobre: la misión, la amenaza y el ciberespacio, proporcionada a los cibercombatientes de forma estructurada y fácilmente visible y comprensible, de manera que apoye el asesoramiento y la toma de decisiones en las operaciones en el ciberespacio. (Winterfeld, 2002).

Este enfoque incluye la realización de un análisis detallado del entorno, similar al proceso de Planeamiento basado en Inteligencia (*Intelligence Preparation of the Battlefield*, IPB) (U.S. Department of the Army, 2009). Algunos de los conceptos claves traducidos al ámbito de las operaciones en el ciberespacio son:

- Bases de Partida: serán puntos de entrada del atacante (tales como, correos electrónicos, puertos USB, interconexiones entre sistemas y servicios, etc.).
- Objetivos: serán servicios o activos críticos que el adversario puede tener intención de atacar o alcanzar (tales como, servidores de bases de datos, Servidores de aplicaciones críticas, servidores de servicios CORE, servicios COI[17] y servicios básicos, etc.).
- Avenidas de Aproximación[18]: serán las rutas más vulnerables dentro del ciberespacio a defender[19] que puede ser empleados por un atacante en su avance hacia sus objetivos.

[15] En función de la coyuntura geopolítica, de la misiones y operaciones, etc.
[16] Atacar sus recursos humanos, tecnológicos, formativos, económicos, etc.
[17] COI son las siglas que se corresponde con: «Community of Interest». Son servicios funcionales como INTEL-FS, JTS, etc. (anteriormente se denominaban Servicios FAS o Funtional Area Services).
[18] El número de «Avenidas de Aproximación» potenciales puede ser numerosos, por lo que es necesario realizar un análisis y descartar aquellas cuyas vulnerabilidades no sean, teóricamente, explotables por las TTP de los actores de la ciberamenaza definido para cada caso. Además, estas rutas deberán priorizarse desde un punto de vista de planeamiento de la defensa y bloqueo de dichas rutas.
[19] Se entiende por «Ciberespacio a defender», al conjunto de sistemas IT y OT que soportan las capacidades militares y por tanto las operaciones militares.

— Zonas Ocultas o Semi-Ocultas: serán zonas del ciberespacio a defender donde los adversarios pueden operar sin ser detectados por los sistemas tradicionales de ciberseguridad. Pueden ser:

  - Zonas Ocultas: serán zonas del ciberespacio a defender no monitorizada por mecanismos de ciberseguridad de detección.
  - Zonas Semi-Ocultas: serán zonas del ciberespacio a defender que, aunque monitorizados por mecanismos de detección, estos dispositivos no disponen de las reglas de detección o la configuración adecuada para detectar las TTP[20] empleadas por los actores de la ciberamenazas específicos a la que nos enfrentamos.

— Zonas a Cubierto: serán zonas del ciberespacio a defender sin mecanismos de ciberdefensa y ciberseguridad implementados que nos permitan reaccionar directamente sobre el atacante o modificar la configuración[21] del ciberespacio.

— Terreno Clave Ciber (CKT[22]): serán puntos del ciberespacio a defender (normalmente donde convergen rutas críticas y vulnerables, como interconexiones de sistemas, servidores esenciales, satélites o cables submarinos), cuyo control, defensa y monitorización proporciona una ventaja defensiva.

  El Terreno Clave (CKT) son aquellas zonas del ciberespacio que, si son defendidos de forma adecuada, dificultarán enormemente el progreso o avance del adversario por nuestro ciberespacio y el éxito de los ataques del adversario sobre sus objetivos en el ciberespacio. (Multinational Capability Development Campaign, 2017).

Este análisis ayuda a planificar una defensa proactiva y dinámica, anticipando los movimientos del adversario y cerrando brechas antes de que puedan ser explotadas.

3.4.1 Cyber-IPB: objetivos y beneficios

El Cyber-IPB permite:

— Identificar quién podría atacarnos, qué podría atacar, por qué y cómo.

[20] TTP son las siglas que se corresponden con: «Tactics, Techniques, and Procedures». (Tácticas, Técnicas y Procedimientos).
[21] Por ejemplo, modificando la configuración de seguridad de los dispositivos o las reglas de acceso, etc.
[22] CKT son las siglas que se corresponden con: «Cyber Key Terrain». Terreno Clave en el Ciberespacio. Equivalente al concepto de «Terreno Clave» en el ámbito terrestre pero trasladado al ámbito del ciberespacio.

— Detectar rutas de ataque y zonas críticas explotables por el adversario:
  - Rutas vulnerables dentro del ciberespacio.
  - Vulnerabilidades explotables en el ciberespacio.
  - Configuraciones inseguras explotables.
— Evaluar impactos potenciales y riesgos (técnicos, tácticos y operacionales).
— Diseñar planes defensivos, de prevención, contención, reacción y recuperación más eficaces y eficientes.

Todo esto con el fin de:

— Anticiparse al adversario.
— Asignar mejor los escasos recursos existentes:
  - Priorizar recursos
  - Priorizar actividades defensivas
  - Priorizar zonas del ciberespacio donde ejercer los esfuerzos principales en el ciberespacio.
— Reducir el impacto operativo de un posible ciberataque.

3.5 Planes de ciberdefensa (Corletti Estrada, 2017)

Con base en este análisis Cyber-IPB, se elaborará un Plan de Ciberdefensa específico, cuyo objetivo es:

— Reducir los riesgos en el ciberespacio.
— Reducir los potenciales impactos.
— Responder a los ciberataques.
— Garantizar la continuidad operativa.
— Asegurar el cumplimiento de la misión.

Se diseñarán y ejecutarán planes de ciberdefensa en todos y cada uno de los niveles de la guerra: técnico, táctico, operacional y estratégico. Cada uno de los planes de estos niveles hará frente a la ciberdefensa desde perspectivas diferentes:

— Nivel Técnico: gestión técnica de los riesgos y de los potenciales impactos.
— Nivel Táctico: dirección de la ciberdefensa de forma táctica, como una defensa del ciberespacio como un todo.

— Nivel Operacional: apoyo a la gestión de los riesgo e impactos de ciberataques en las operaciones militares.

— Nivel Estratégico: gestión estratégica de recursos de ciberdefensa (humano, formativos y tecnológicos), ataque estratégico a las fuentes de las capacidades ofensivas del adversario

Este plan incluye los siguientes componentes:

3.5.1 Plan de Detección Avanzada

Tiene como propósito establecer mecanismos que permitan identificar comportamientos maliciosos en redes y sistemas, usando inteligencia sobre ciberamenazas.

Se centra en:

— Desplegar sensores de seguridad en áreas clave del ciberespacio (Cy-NAIs[23]), en especial, en puntos estratégicos[24] por donde podría avanzar un adversario.

— Configurar estos sensores con reglas que permitan detectar tácticas, técnicas, herramientas y *malware* habitualmente usados por los actores de amenazas definidos, según inteligencia de ciberamenazas táctica y técnica.

3.5.2 Plan de Obstáculos

Busca dificultar el avance del adversario dentro del sistema a través de:

— Mecanismos de seguridad que monitorean, filtran y restringen el tráfico de datos en puntos clave del ciberespacio, impidiendo el libre movimiento del adversario.

— Planes predefinidos para desactivar servicios[25] vulnerables que podrían ser aprovechados como vía de acceso, penetración y progresión de un ciberataque.

Este plan se basa en un análisis detallado de las posibles rutas de ataque (Avenidas de Aproximación), considerando las debilidades (vulnerabilidades) del sistema y las capacidades (TTPs y tecnología) del enemigo.

[23] CyNAI son las siglas que se corresponden con: «Cyber Name Areas of Interest».
[24] Generalmente, puntos de confluencia de varias avenidas de aproximación del adversario.
[25] Sería el equivalente a la realización de destrucción de puentes en un avance adversario en al ámbito terrestre, para retrasarlos o canalizarlos.

3.5.3 Plan de Mitigación de Efectos

Diseñado para minimizar los daños (efectos/impactos) en caso de un ciberataque exitoso por parte del adversario:

— A nivel táctico, se establecerán sistemas redundantes y configuraciones de alta disponibilidad que mantengan los servicios activos pese a las agresiones.

— A nivel operacional, se implementarán planes de contingencia con recursos alternativos, tanto militares como civiles, que aseguren la continuidad de las operaciones, incluso fuera del ámbito digital[26].

3.5.4 Plan de Reacción

Contempla respuestas específicas frente a distintos tipos de ciberataques anticipados (Cy-OCOAs[27]), incluyendo:

— Planes de despliegue de Unidades de Reacción Rápida (RRT[28]).

— Planes detallados de gestión de incidentes a nivel técnico y táctico.

3.5.5 Plan de Recuperación

Asegura la restauración rápida de servicios y sistemas críticos mediante:

— En el ámbito IT y OT, el uso de tecnologías como la virtualización o hiperconvergencia[29], que permiten reconstruir servicios en minutos.

— En cuanto a datos, sistemas de recuperación de datos (DRP[30]) con tiempos (RTO[31]) y puntos de recuperación (RPO[32]) definidos según la criticidad[33] del servicio para la operación militar.

---

[26] Por ejemplo, tener previsto transporte de combustible mediante trenes de cisternas de combustible, en caso de que un determinado oleoducto sea atacado.

[27] Cy-OCOA son las siglas que se corresponden con: «Cyber Opposite Course of Action». Líneas de acción potenciales de las operaciones en el Ciberespacio del adversario.

[28] RRT son las siglas que se corresponden con: «Rapid Reaction Team». Equipo de Reacción Rápida ante incidentes de Ciberseguridad o Ciberataque.

[29] Se trata de sistemas avanzado que, en vez de tener servidores, almacenamiento (como SAN o NAS) y redes separados; la infraestructura hiperconvergente (HCI) combina todo eso en nodos modulares (como cajas que tienen de todo un poco), lo que facilita la escalabilidad y el manejo del entorno.

[30] DRP son las siglas que se corresponden con: «Data Recovery Plans».

[31] RTO son las siglas que se corresponden con: «Recovery Time Objective», es decir, el tiempo máximo en el que se debe poder recuperar los datos y que el servicio o sistema pueda acceder a los datos.

[32] RPO son las siglas que se corresponden con: «Recovery Point Objective», es decir, el tiempo máximo de datos que se puede perder, que corresponde al tiempo que transcurre entre que se realizan dos *backups* de datos consecutivos.

[33] Impacto potencial en las operaciones en caso de ataque al mismo.

4 Desafíos Tecnológicos en Ciberdefensa

El panorama actual del ciberespacio está marcado por una evolución acelerada de las amenazas. Ataques como los *zero-day*[34], el *malware* polimórfico[35] o el ransomware dirigido, avanzan a una velocidad que supera la capacidad de respuesta de las herramientas de ciberseguridad tradicionales. (Internet Security Auditors, 2025).

Los mecanismos convencionales, basados en firmas o indicadores técnicos de compromiso (IOC), han quedado obsoletos frente a adversarios altamente cualificados, sofisticados y, en muchos casos, respaldados por estados hostiles.

4.1 Necesidad de soluciones nacionales y estratégicas

Ante este contexto, se vuelve esencial contar con sistemas de ciberdefensa diseñados específicamente para este entorno de alta exigencia y estén adaptadas a las necesidades específicas de nuestras Fuerzas Armadas.

Además, por su carácter estratégico[36], es fundamental que estas soluciones:

— Sean desarrolladas a nivel nacional, garantizando la independencia tecnológica.

— No dependan de tecnologías o empresas extranjeras que puedan comprometer la seguridad o deshabilitar las capacidades defensivas remotamente (*Kill-Switch*[37]).

---

[34] Un «zero day» (o «día cero») es una vulnerabilidad de seguridad en software que es descubierta por atacantes antes de que el desarrollador del software sepa que existe. Como el fabricante no ha tenido tiempo de corregirla (porque no sabía de ella), no hay parches ni defensas oficiales disponibles, lo que la hace especialmente peligrosa. Su nombre proviene del hecho que el proveedor del ***software*** tiene «cero días» para arreglarla desde que se descubre públicamente o se empieza a explotarse por potenciales adversarios u actores maliciosos.

[35] Capaz de cambiar su forma para evadir la detección.

[36] La ciberdefensa es un ámbito tan transversal a todas las capacidades militares, lo cual le proporciona un carácter estratégico y requiere, por tanto, de una independencia estratégica, no se puede depender de tecnología no nacional. La ciberdefensa de nuestras capacidades militares no puede depender de una industria bajo control de un tercer país, que pueda desactivar estas capacidades de ciberdefensa a su antojo, o que pueda acceder a información sobre las debilidades de nuestro ciberespacio.

[37] Un *Kill-switch* (o interruptor de apagado de emergencia) es un mecanismo diseñado para detener de manera automática un sistema, proceso o dispositivo en caso de emergencia o cuando se detecta una amenaza. Un *Kill-switch* puede apagar remotamente una ***app*** o dispositivo si es robado o comprometido o a voluntad. Por ejemplo, algunos ***smartphones*** permiten borrar todos los datos si se pierden.

La industria nacional de ciberdefensa se convierte así en un pilar clave para garantizar una defensa autónoma y eficaz del ciberespacio militar. Sin una base tecnológica soberana, la ciberdefensa se convierte en un castillo con cimientos prestados: estable, mientras el proveedor de las herramientas de ciberdefensa lo permita. Fortalecer la industria nacional no es una opción, es una necesidad estratégica. (Arteaga y Alonso, 2023)

4.2 Necesidad de desarrollos y adquisiciones ágiles

El ciberespacio es un entorno dinámico, donde atacantes y defensores compiten en una carrera tecnológica continua. Por ello, las herramientas de ciberdefensa deben:

— Mantenerse a la par o por delante del ritmo tecnológico de los atacantes.

— Superar los tiempos lentos de adquisición y desarrollo típicos en entornos tradicionales.

— Tener ciclos de evolución y despliegue muy rápidos[38].

4.3 Lagunas Tecnológicas

A pesar de los avances, siguen existiendo lagunas tecnológicas importantes, especialmente en tres áreas críticas:

1. Inteligencia de ciberamenazas.
2. Conciencia situacional.
3. Mando y Control de operaciones defensivas.

4.3.1 Conciencia Situacional (CySA[39])

Uno de los principales retos es contar con una visión clara, completa, precisa y en tiempo real de lo que acontece en el ciberespacio. Sin esta Conciencia Situacional, resulta difícil:

— Gestionar riesgos en el ciberespacio.

— Priorizar activos a defender y acciones a ejecutar.

— Entender el contexto de un ciberataque.

— Evaluar su impacto potencial y efectos operativos.

— Tomar decisiones informadas bajo presión.

[38] Es decir, ciclos de vida de las herramientas y software específico de ciberdefensa muy ágil.
[39] CySA son las siglas que se corresponde con: «Cyber Situational Awareness».

Esto implica monitorizar enormes volúmenes de datos en tiempo real, provenientes de múltiples fuentes, y transformarlos en información útil. Para lograrlo, se necesita:

— Integración de datos desde diversos sistemas y fuentes.

— Un repositorio único, flexible y escalable (*datalake*).

— Herramientas avanzadas de procesado y análisis en tiempo casi real.

— Interfaces que presenten la información de forma personalizable[40] a las necesidades de cada combatiente en el ciberespacio en cada rol y nivel de mando.

4.3.2 Modelado de la ciberamenaza

Frente a amenazas genéricas, el entorno actual requiere una inteligencia especializada y orientada a actores concretos. El modelado de amenazas se ha convertido en un elemento central en los sistemas modernos de Inteligencia de ciberamenazas y esencial para una táctica y estrategia avanzada de ciberdefensa.

El modelado de la ciberamenaza consiste en:

— Recopilar, almacenar, analizar y representar toda la información disponible sobre cada actor de la amenaza.

— Construir perfiles estructurados (atributos y parámetros) que incluyan: tácticas, herramientas, objetivos frecuentes, infraestructura, relaciones geopolíticas, capacidades técnicas, etc.

— Establecer una especie de «ficha policial digital» de cada actor, con sus huellas, modus operandi (TTP), relaciones, patrones y comportamientos.

— Buscar relaciones y patrones entre los datos de la ciberamenaza.

— Representar gráficamente el modelado de la amenaza de forma entendible por los analistas de Inteligencia de ciberamenazas.

El modelado de la ciberamenaza se aplica a:

— Planeamiento: predicción y anticipación a los comportamientos de los actores de la ciberamenazas para reducir riesgos y definir planes de contingencia.

— Conducción de operaciones (Gestión de Incidentes):

[40] Mediante filtrado y selección del formato de representación más adecuado en cada momento y para cada finalidad.

- Compara[41] características[42] (modelado) del incidente con las del actor.
- Establece atribuciones probables.
- Dirige la investigación.
- Propone tácticas y contramedidas adaptadas.

El modelado de la amenaza permitirá:

— Realizar atribuciones técnicas y tácticas sobre la posible autoría de los incidentes, asignando probabilidades basadas en la coincidencia entre los patrones del incidente y los comportamientos conocidos de distintos actores de ciberamenazas.

— Orientar la investigación del incidente utilizando inteligencia de ciberamenazas, definiendo líneas de investigación en función de los modos de operación (*modus operandi*) de las posibles atribuciones (autores potenciales) identificados en el paso anterior.

— Anticipar los próximos movimientos del atacante, basándose en su perfil y comportamiento histórico.

— Definir las tácticas y técnicas más adecuadas para responder al incidente, incluyendo acciones de detección, contención, mitigación, reacción y recuperación, con el objetivo de recuperar el control del sistema y expulsar al adversario.

La dificultad técnica radica en desarrollar sistemas capaces de combinar grandes volúmenes de datos con técnicas de inteligencia artificial (IA) (como el *Machine Learning* (ML) o *Deep Learning* (DL), para identificar patrones y relaciones útiles que permiten guiar la ciberdefensa (*Intel Driven Defensive Cyber Operations*).

En el ámbito de las operaciones en el ciberespacio[43], una forma tecnológicamente avanzada es representar a los atacantes a través del modelado vectorial. Esta técnica utiliza bases de datos vectoriales en las que cada actor de amenaza se representa como un punto en un espacio multidimensional[44]. Cada una de esas dimensiones corresponde a una característica o

[41] Esta comparación se realiza de forma matemática (automatizada), mediante comparación vectorial de los vectores (en una base de datos vectorial) que representan cada uno de los incidentes y de los actores, en las que, por ejemplo, cada actor es representado por un vector multidimensional y en el que cada dimensión de ese espacio vectorial es un parámetro o atributo de estos.

[42] Haciendo un símil, es como comparar la ficha de investigación policial (modelado) de un incidente o robo (con sus evidencias e indicios) con fichas policiales (modelado) de los delincuentes.

[43] Especialmente, en cuanto a gestión de incidentes y análisis de inteligencia.

[44] Con múltiples dimensiones, cada una de ellas representando un parámetro o característica del objeto a modelar.

comportamiento del atacante y el conjunto de estos datos forma un vector que lo describe.

Este enfoque no solo sirve para modelar actores maliciosos, sino que también se puede aplicar a otros elementos del ciberespacio, como incidentes de seguridad o ciberataques.

Si representamos un ciberataque como un vector en ese mismo espacio multidimensional, puede compararse con los vectores de los distintos actores de amenaza.

Una comparación entre el vector del ataque y el del posible autor (actor de amenaza) permite obtener un «vector diferencia». Este «vector diferencia» revela qué características del atacante aún no se han manifestado en el potencial ciberataque en curso, lo que ofrece dos ventajas clave:

— Guía de investigación: orienta sobre las evidencias, comportamientos o detalles que deberían buscarse en el análisis del ciberataque.

— Predicción de acciones futuras: ayuda a anticipar los siguientes movimientos del atacante, basándonos en lo que normalmente haría, pero aún no ha hecho.

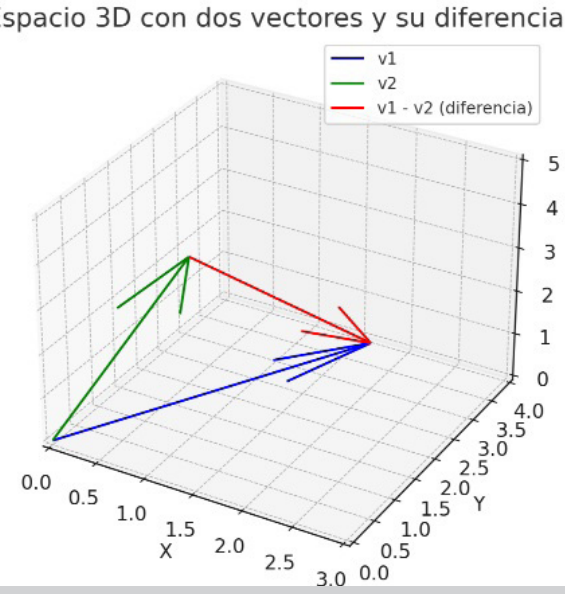

Figura 1. Modelado en tres dimensiones. Representación de vectorial de dos objetos modelados vectorialmente en un cubo tridimensional (de solo tres parámetros) y la representación del vector diferencia de la comparación de los dos modelos. Las proyecciones de ese vector diferencia en los ejes de dicho cubo, nos mostrará los parámetros en los que ambos modelos no concuerda, y el valor de esa diferencia. En un modelado real, el cubo no sería tridimensional, sino n-dimensional. [Imagen obtenida de Chagpt]

Además, al comparar el vector de un ataque con los vectores de múltiples actores conocidos, se puede realizar un análisis probabilístico de atribución. Cuanto más cercano sea un vector a otro (menor distancia entre ellos), mayor será la probabilidad de que el actor correspondiente sea el responsable del ataque.

Este tipo de técnicas ofrece un enorme potencial no solo en ciberdefensa, sino también en otras áreas donde es necesario analizar y anticipar comportamientos complejos.

5 Iniciativas tecnológicas impulsadas por el MCCE

El incremento constante de amenazas en el ciberespacio ha obligado a desarrollar soluciones tecnológicas específicas para la ciberdefensa militar. Sin embargo, la oferta comercial en este ámbito aún es escasa, debido a la naturaleza reciente del enfoque militar en este dominio.

Por ello, el Mando Conjunto del Ciberespacio (MCCE) ha promovido una serie de proyectos que buscan cubrir estas carencias tecnológicas mediante herramientas tecnología y conceptualmente avanzadas, diseñadas para:

- Integrar Inteligencia de Ciberamenazas.
- Proporcionar capacidades de Mando y Control.
- Mejorar la Conciencia Situacional.
- Asegurar la Respuesta Defensiva operativa.

A continuación, se presentan las principales iniciativas.

5.1 Plataforma PICO

La plataforma PICO (Plataforma de Inteligencia para la Conducción de Operaciones en el Ciberespacio) ha representado uno de los primeros pasos de adquisición y evolución de capacidades específicas de ciberdefensa militar dentro del MCCE.

Se basa en el desarrollo previo del producto CIAT[45] de la empresa Telefónica Soluciones de Criptografía (TELCRYP, Grupo Telefónica) y ha sido adaptada para fines militares por dicha compañía para cumplir con los requisitos operativos definidos y requeridos por el MCCE.

5.1.1 ¿Qué ofrece PICO?

PICO combina dos capacidades en una única solución:

- Gestión de inteligencia de ciberamenazas.
- Gestión de incidentes de ciberseguridad.

[45] CIAT son las siglas que se corresponde con: «Plataforma Global de Ciber Inteligencia Avanzada de Telefónica».

Esta integración permite:

— Modelar incidentes y actores de amenazas.
— Correlacionar evidencias entre ambos modelos (incidentes y amenazas).
— Gestionar ciberataques dirigidos por inteligencia de ciberamenazas.
— Priorización, automatización y control de tareas de respuesta a ciberataques o incidentes de seguridad.

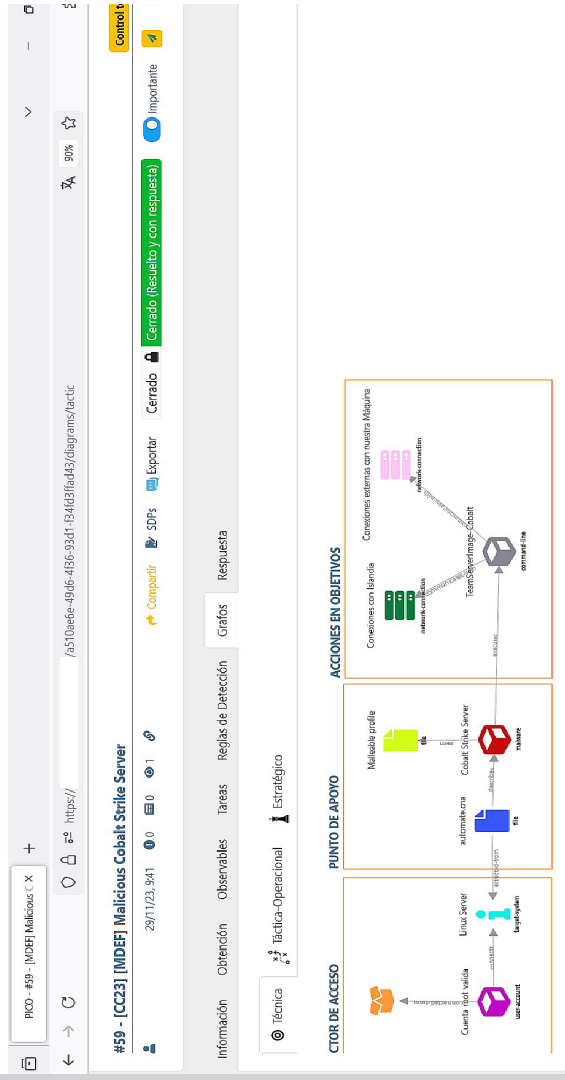

Figura 2. Modelado Técnico de un Ciberataque. Esta imagen muestra un caso de modelado de un Ciberataque realizado mediante la Plataforma PICO. En el que se representa los pasos, evidencias y artefactos empleados por un atacante en la ejecución de su ataque. [Imagen cedida por la empresa Telefónica Soluciones de Criptografía (TELCRYP, Grupo Telefónica)]

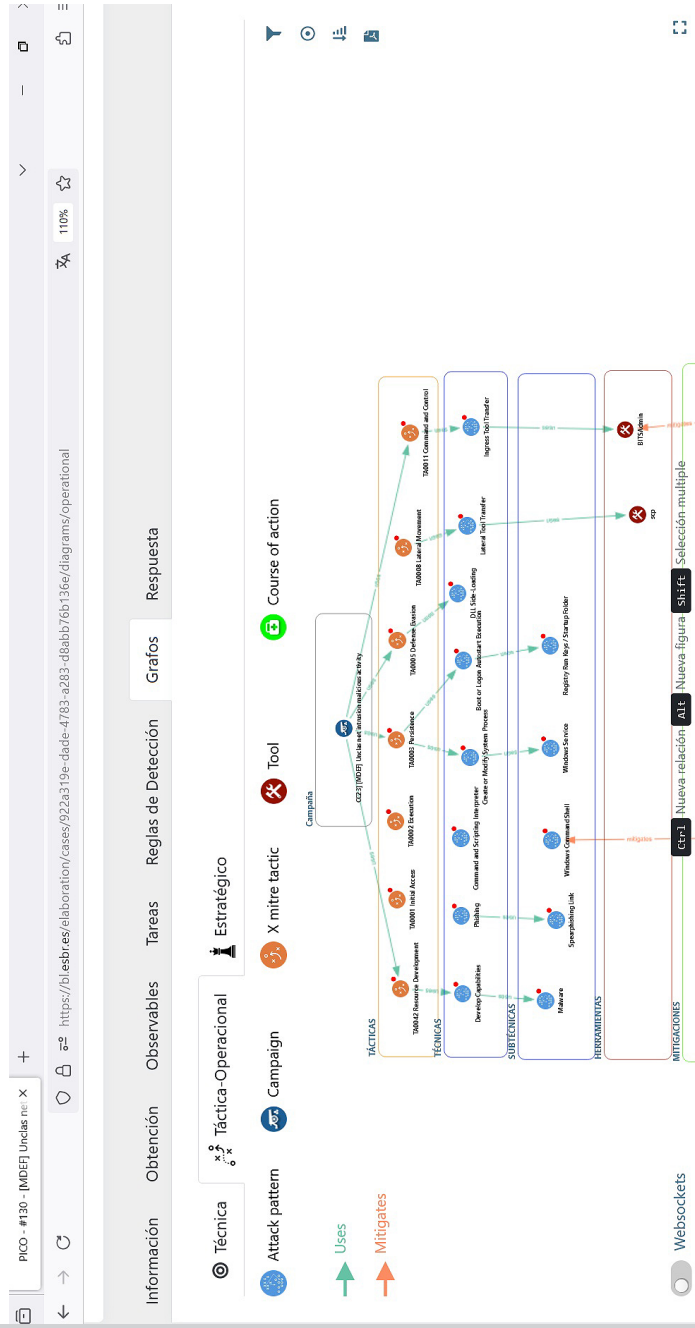

Figura 3. Modelado Táctico de un Ciberataque. Esta imagen muestra un caso de modelado Táctico de un ciberataque, realizado mediante la Plataforma PICO. En el que se representa las tácticas, técnicas, procedimientos, herramientas malware empleados, así como las COAs defensivas empleadas por el Ciberdefensor. [Imagen cedida por la empresa Telefónica Soluciones de Criptografía (TELCRYP, Grupo Telefónica)]

Además, PICO emplea el *framework* de las matrices de MITRE ATT&CK[46] para modelar (mapear) las tácticas, técnicas y procedimientos empleadas por los atacantes, lo que permite realizar atribuciones más precisas y planes de defensa proactivas.

La plataforma PICO está diseñada para facilitar una gestión integral, coordinada y eficiente de las operaciones defensivas y de inteligencia, a nivel técnico (e incipientemente a nivel táctico), en el ámbito del ciberespacio. Estas son sus principales capacidades:

— Unificación de herramientas: permite operar desde una única plataforma, eliminando, en gran medida, la necesidad de usar múltiples sistemas a la vez. Esto ofrece un cuadro de mando centralizado que simplifica la gestión y mejora la eficiencia.

— Gestión centralizada de la información de inteligencia de ciberamenazas: reúne todos los datos disponibles tanto del entorno propio como de posibles amenazas en un repositorio único[47], lo que facilita la correlación de información y mejora la conciencia situacional para apoyar una toma de decisiones más efectiva.

— Automatización: optimiza tareas repetitivas relacionadas con la gestión de incidentes y el análisis de inteligencia y permite a los operadores centrarse en labores de mayor valor estratégico. Permite también definir *workflows* de tareas, con asignación y control de tareas.

— Vigilancia y monitorización integrales: integra diversas herramientas de detección en una sola plataforma, lo que permite una vigilancia continua del ciberespacio, así como una visualización técnica/táctica unificada. Todas las alertas se muestran en una única interfaz, priorizadas según el nivel de amenaza identificado por la inteligencia de ciberamenazas y la misión.

— Sincronización entre inteligencia y operaciones: asegura que la gestión de incidentes esté guiada por inteligencia (Intel Driven), lo que permite responder de forma más eficaz ante ciberataques y anticipar posibles movimientos del adversario.

— Correlación de datos: la plataforma analiza de forma automatizada grandes volúmenes de información para detectar patrones y

[46] Para hacer un símil, las matrices de Mitre Att&ck son a Ciberdefensa lo que la tabla periódica de elementos es a la química. Es decir, las matrices de Mitre Att&ck es una especie de tabla periódica ordenada de todas las tácticas, técnicas y procedimientos existentes o al menos identificadas.

[47] Se trata de una base de datos relacional. No incorpora aún un ***datalake*** y, por tanto, no presenta las ventajas de este tipo de tecnologías.

relaciones entre incidentes, lo que ayuda a identificar conexiones entre ataques en apariencia aislados.

— Gestión y respuesta efectiva a incidentes: permite registrar, clasificar y priorizar incidentes según su impacto potencial, asignar recursos de manera eficiente, y coordinar respuestas con rapidez, al estilo de los sistemas SOAR[48].

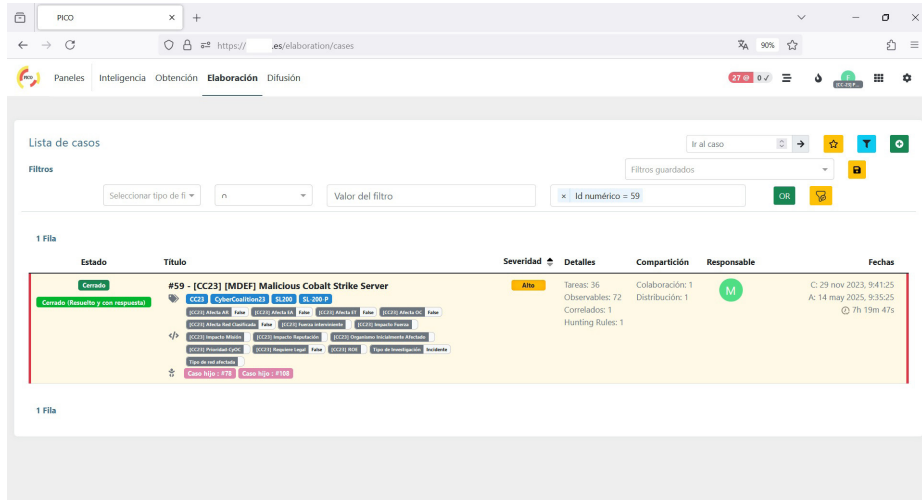

Figura 4. Visualización de la Vista de Gestión de Incidentes de la Plataforma PICO. [Imagen cedida por la empresa Telefónica Soluciones de Criptografía (TELCRYP, Grupo Telefónica)]

— Apoyo a la toma de decisiones: genera información procesada y relevante para que los equipos de ciberdefensa puedan actuar con rapidez y precisión, incluso bajo presión.

— Reducción de riesgos: contribuye a mitigar los efectos de los incidentes y a prevenir futuras amenazas, de modo que asignan y coordinan las tareas defensivas de forma estructurada y eficaz.

Al tomar como punto de partida esta versión de PICO inicial, desde el MCCE se planea apoyar de forma activa la evolución de este producto hasta convertirse en un módulo táctico/técnico del Sistema de Inteligencia y del Sistema de Mando y Control dentro del futuro SCOMCE[49].

[48] SOAR son las siglas que se corresponde a «Security Orchestration, Automación and Response». Se trata de un dispositivo de gestión de incidentes de seguridad con capacidad de respuesta automatizada y de *workflow*.

[49] SCOMCE son las siglas que se corresponden con: «Sistema de Combate en el Ciberespacio».

5.2 ECYSAP / ECYSAP EYE

El proyecto ECYSAP (European Cyber Situational Awareness Platform) nace de una iniciativa europea impulsada y subvencionada por la UE, con el objetivo de desarrollar una plataforma de Conciencia Situacional (en su versión v 1.0) y de Mando y Control de operaciones de ciberdefensa (en su versión v 2.0).

5.2.1 ECYSAP[50] v1.0

Figura 5. Visualización del logo del proyecto ECYSAP. [Imagen cedida por la empresa INDRA]

Se trata de una herramienta centrada en proporcionar Cyber Situational Awareness (CySA).

- Desarrollado con apoyos de fondos europeos.
- Coordinado por INDRA, con participación de España, Italia, Francia y Estonia.
- El MCCE (Mando Conjunto del Ciberespacio) ha apoyado este proyecto desde el punto de vista técnico y operativo, por delegación de la DGAM, desde sus inicios.
- La OTAN ha mostrado su interés en esta herramienta y a nivel de la UE se ha presentado en la reunión Anual de Cybercommanders de la UE de este año. Las FAS españolas cuentan con disponer de una versión de ECySAP adaptada a las necesidades de nuestras FAS como producto operativo y funcionando antes de final de año (2025) en las instalaciones del MCCE.

ECySAP dispone de cuatro niveles de visualización, correspondientes a los niveles de la guerra: técnico, táctico, operacional y estratégico.

Cada nivel de la guerra, a su vez integra cuatro vistas especializadas:

- Vista Misión: enfocada a satisfacer las necesidades del personal del área de operaciones y planes.
- Vista Amenaza: enfocada a satisfacer las necesidades del personal del área de inteligencia.
- Vista Ciberespacio enfocada a satisfacer las necesidades del personal del área CIS/CYBER.

[50] ECySAP son las siglas que se corresponden con: «European Cyber Situational Awareness Project».

— Vista CYBER: enfocada a satisfacer las necesidades del comandante CYBER o comandante de las operaciones.

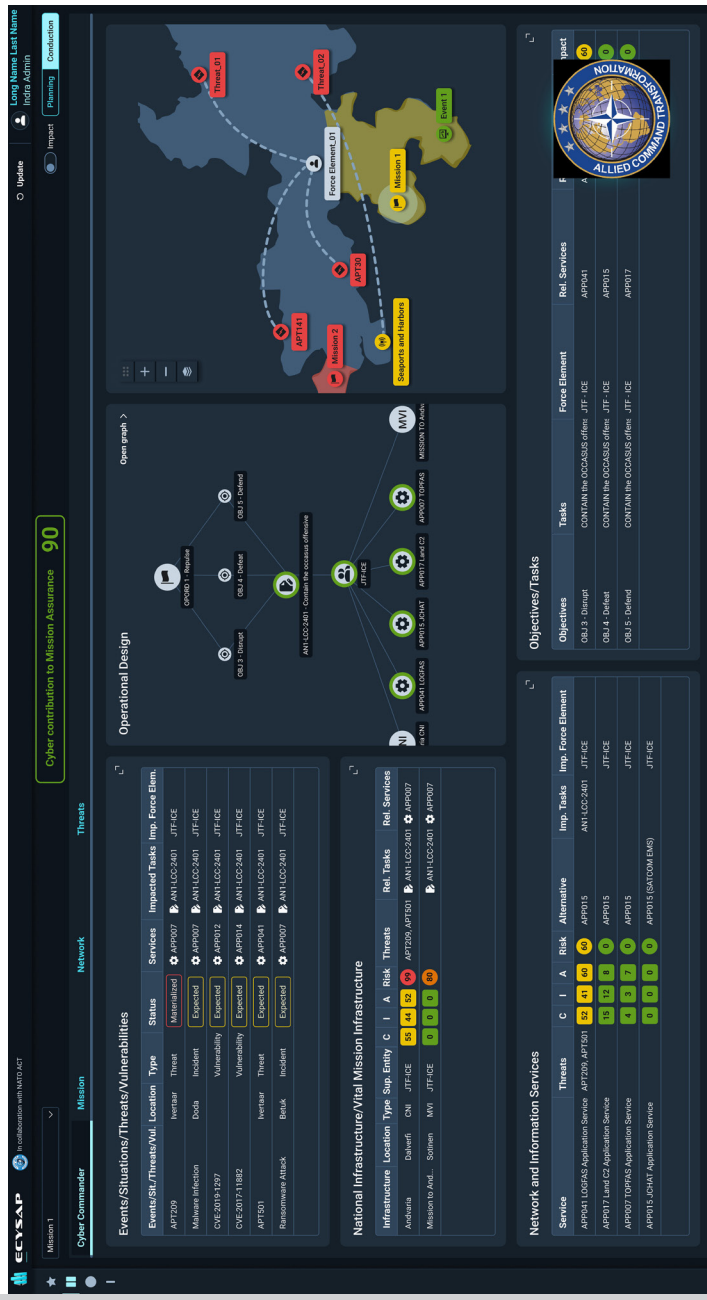

Figura 6. Visualización de la Plataforma ECYSAP.(Vista de nivel Operacional) para el Oficial de Enlace o Jefe del Grupo de trabajo Ciberoperaciones (CyOWG) en un nivel de Mando Conjunto. [Imagen cedida por la empresa INDRA y NATO ACT CYBER]

Figura 7. Visualización de la Plataforma ECYSAP (Vista de nivel Táctico) para el Oficial de Inteligencia de Ciberamenazas dentro del Estado Mayor de un Mando de Operaciones en el Ciberespacio. En el que puede visualizar y editar las TTPs de un Actor de la Ciberamenaza concreto. [Imagen cedida por la empresa INDRA y NATO ACT CYBER]

5.2.2 ECYSAP v2.0 (ECYSAP EYE)

Versión evolutiva del sistema ECYSAP v 1.0, cuyo objetivo es convertirse en un Sistema Integral de Mando y Control de operaciones en el ciberespacio, incorporando:

— Conciencia Situacional (CySA).
— Planificación y Conducción de operaciones y misiones en el ciberespacio (Guiadas por inteligencia de ciberamenazas).
— *Wargaming* y simulación[51].
— Flujo de trabajo colaborativo.
— *Targeting*.

Este proyecto, también es subvencionado por la UE y será desarrollado por un consorcio de ocho países europeos[52], liderado de nuevo por INDRA y está previsto su finalización para 2028, en nivel de madurez tecnológica TRL 6-7[53].

El MCCE (Mando Conjunto del Ciberespacio) también apoyará este proyecto desde el punto de vista técnico y operativo, por delegación de la DGAM.

5.3 SCOMCE: sistema de Combate en el Ciberespacio

Como parte de su esfuerzo por reforzar su capacidad de combate en el ciberespacio, el MCCE está desarrollando el Sistema de Combate en el Ciberespacio (SCOMCE).

El sistema SCOMCE es el proyecto[54] más ambicioso del MCCE. Se plantea como un «Sistema de Sistemas» que integre capacidades completas para operar y combatir en el ciberespacio, con la inclusión los siguientes sistemas:

— Sistema de Mando y Control:
  • Proporciona la capacidad de dirección y supervisión de las operaciones en el ciberespacio en tiempo real.

[51] Con base en «Modelados» de los diferentes actores de la ciberamenaza. Estos modelados se emplearán para las simulaciones de los ataques de los actores de la ciberamenaza en módulos de ***wargaming*** de nivel técnico (simulaciones LIVE) y nivel táctico (simulaciones de carácter TTX).
[52] Francia, Austria, Italia, Estonia, Polonia, Rumania, Grecia y España.
[53] TRL siglas que se corresponden con: «Tecnology Readiness Levels» (Nivel de madurez tecnológica). TRL 6 – Tecnología demostrada en un entorno relevante (entorno relevante a nivel industrial en el caso de tecnologías habilitadoras clave). TRL 7 – Demostración del prototipo del sistema en un entorno operativo.
[54] En realidad, se tratará de un programa compuesto por casi una veintena de proyectos.

— Sistema de Inteligencia:

  - Proporciona la capacidad de inteligencia de ciberamenazas en todos los niveles de la guerra (técnico, táctico, operacional y estratégico).

— Sistema Ofensivo:

  - Proporciona la capacidad de ejecutar operaciones activas en el ciberespacio adversario y permite acciones de disuasión, neutralización, etc.

— Sistema Defensivo:

  - Proporciona las capacidades de ciberdefensa del ciberespacio propio mediante medidas avanzadas de detección, contención, mitigación y recuperación ante ciberataques.

— Sistema Transversal:

  - Proporciona capacidades transversales a todos los sistemas anteriores: servicios compartidos y soporte a los demás sistemas.

La inclusión de un Sistema de Inteligencia propio dentro del SCOMCE demuestra la importancia creciente de la inteligencia de ciberamenazas como eje central de toda operación defensiva u ofensiva en el ciberespacio, al igual que ocurre en otros ámbitos de operaciones militares.

Este sistema está siendo diseñado para dar servicio en todos los niveles de mando y niveles de la guerra, desde el nivel técnico hasta el estratégico.

6 Requisitos tecnológicos avanzados para el SCOMCE

El Sistema de Combate en el Ciberespacio requiere integrar las tecnologías más avanzadas disponibles para cumplir con los desafíos operativos y estratégicos del dominio o ambiente de operaciones en el ciberespacio.

Se requiere que sea capaz de:

— Centralizar toda la información relevante del ciberespacio.

— Correlar, relacionar y analizar toda la información y datos disponibles de forma estructurada y predictiva.

— Apoyar la toma de decisiones en tiempo real.

Existe cuatro tecnologías que son, sobre todo, críticas para alcanzar las capacidades que requiere el Sistema de Inteligencia del SCOMCE.

6.1 Tecnología de datalake

Los *datalakes* representan una evolución tecnológica respecto a las bases de datos tradicionales, ya sean relacionales o no relacionales, y aportan un valor significativamente superior.

Un datalake[55] es un repositorio único[56] que permite ingestar, almacenar y preprocesar grandes volúmenes de datos de múltiples fuentes y formatos, de forma estructurada o no estructurada.

Entre sus principales ventajas destacan:

— Almacenamiento flexible y versátil: pueden manejar datos en múltiples formatos y niveles de estructura e incluyen:

  • Estructurados (como los almacenados en bases de datos relacionales).

  • Semiestructurados (por ejemplo, archivos JSON o XML).

  • No estructurados (textos, imágenes, capturas de red).

  • Poco estructurados (como datos de sensores o comunicaciones interceptadas).

  Además, permiten guardar la misma información y de forma coherente en diferentes formatos simultáneamente (relacional, gráfico, vectorial, etc.), lo que facilita su consulta por parte de Sistemas de Inteligencia, Mando y Control, u otros sistemas que requieran distintos tipos de análisis.

— Integración de múltiples fuentes: unifican información que, por norma, estaría dispersa en sistemas independientes o «silos de datos». Esta centralización favorece la correlación entre datos de diferentes orígenes y herramientas, lo que ayuda a identificar patrones complejos o relaciones que pasarían desapercibidas en sistemas fragmentados.

---

[55] Un ***datalake*** es un repositorio centralizado que permite almacenar datos en su formato nativo, sin restricciones de estructura o tamaño. En el caso del SCOMCE, este ***datalake*** integrará (a diferencia de las bases de datos tradicionales) todo tipo de información y datos en bruto e incluirá una capa de ***software*** de procesado de datos específico para curar (fusionar, deduplicar, integrar, depurar, enriquecer, relacionar) los datos y la información según las necesidades analíticas del módulo ***software*** posterior del SCOMCE que consuma los datos del ***datalake***.

[56] Actúa como el «repositorio único de la verdad», almacena toda la información y datos (objetos, con sus parámetros/atributos y relaciones semánticas) correspondientes a las operaciones en el ciberespacio. La existencia de silos de información almacenados en distintos sistemas, herramientas y soluciones técnicas dificulta una visión única y clara de la situación en el ciberespacio y la correlación de datos: el descubrimiento de relaciones, patrones y tendencias.

— Preprocesamiento inteligente: antes de almacenar los datos, los *datalakes* pueden realizar tareas como eliminación de duplicados, corrección de inconsistencias y normalización, lo que mejora la calidad y coherencia de la información disponible.

— Escalabilidad: se adaptan fácil al crecimiento del volumen de datos sin necesidad de rediseñar la estructura y permiten almacenar grandes históricos, que son clave para análisis retrospectivos o anticipar tendencias futuras.

— Acceso centralizado: al concentrar toda la información en una única plataforma, se simplifica su gestión y acceso para los equipos de ciberdefensa y mejora la eficiencia operativa y la toma de decisiones.

Este *datalake* se convertirá en el repositorio desde el que los diferentes sistemas del SCOMCE consumirán los datos y la información y en el cual almacenaron los productos generados por los mismos.

6.1.1 Fuentes de información y datos a integrar

El *datalake* debe reunir información detallada y completa que abarque tres grandes áreas clave para la defensa en el ciberespacio:

— La misión: debe incluir misiones, planes, órdenes e informes operativos de todos los niveles de mando y niveles de la guerra. Esto permite analizar cómo dependen las operaciones de ciertas capacidades o servicios del ciberespacio y así identificar los riesgos asociados a posibles ataques que podrían afectar su ejecución.

— La amenaza (organizada por niveles):

- Estratégico: datos sobre actores potenciales, sus alianzas, doctrinas, capacidades, fuentes de financiación, métodos de formación y desarrollo de ciberarmas.
- Operacional: información sobre posibles intenciones, objetivos habituales, efectos que buscan generar y los integrantes que conforman estos grupos o entidades.
- Táctico: conjunto de tácticas, técnicas y procedimientos (TTP) empleados, vectores de entrada, infraestructuras utilizadas, tecnologías, herramientas, *malware* y ciberarmas disponibles.
- Técnico: detalles más específicos sobre las herramientas y *malware* utilizados, vulnerabilidades explotadas y los Indicadores de Compromiso (IOC) que pueden emplearse para detectar sus actividades.

— Información del ciberespacio propio: debe reflejar el estado de los activos y servicios, así como incluir vulnerabilidades, flujos de datos entre ellos, configuraciones de seguridad incorrectas o ausentes, relaciones entre componentes y la ubicación/configuración de los mecanismos de ciberseguridad y ciberdefensa.

La integración total de estos datos permite elaborar una visión única y compartida del ámbito de las operaciones en el ciberespacio (RCyP[57]).

6.1.2 Estructura del *datalake*

Un *datalake* de este tipo está, normalmente, estructurado en las siguientes áreas o zonas:

— Área Bronce: almacena los datos en bruto tal y como llegan.

— Área Plata: organiza los datos según una ontología específica del ciberespacio (relaciones entre activos, amenazas, misiones, etc.).

— Área Oro: almacena datos preprocesados listos para ser utilizados por sistemas de análisis e inteligencia artificial.

6.1.3 Desafío en la implementación de un *datalake*

El verdadero reto para implementar un *datalake* no es tanto tecnológico —hoy en día integrar diferentes fuentes de datos no representa una gran dificultad técnica—, sino más bien cultural y organizativo.

Para que este sistema sea de verdad eficaz, es fundamental que se integren datos provenientes de múltiples ámbitos:

— Los sistemas que gestionan el ciberespacio operativo, controlados por proveedores de servicios IT y OT.

— Los sistemas de Mando y Control (incluido los de planeamiento) en todos los niveles de la guerra y niveles de mando.

— Los sistemas de inteligencia sobre ciberamenazas militares, en los que se incluye, idealmente, información compartida desde organismos civiles, entidades privadas y administraciones públicas.

Sin embargo, esta integración, a menudo, se ve obstaculizada por una falta de comprensión del valor estratégico de la ciberdefensa y de la importancia de centralizar toda la información en una única plataforma que apoye tanto la inteligencia como la toma de decisiones en operaciones del ciberespacio.

[57] RCyP son las siglas que se corresponden con: «Recognized Cyber Picture».

6.2 Ontología

A diferencia de otros tipos de repositorios, un *datalake* requiere del desarrollo de un modelado de datos especifico, ya que no solo define los elementos clave (objetos o conceptos) del dominio, sino también sus atributos, relaciones y reglas que describen cómo interactúan entre sí. Este modelado de datos especifico se denomina «ontologías».

Una ontología es una representación formal y estructurada[58] del conocimiento dentro de un dominio específico, que permite modelar el conocimiento de una forma que puede ser entendida por humanos y procesada por máquinas, lo que la hace especialmente útil en áreas como la inteligencia artificial para realizar inferencias, la gestión del conocimiento, los sistemas expertos o la interoperabilidad entre sistemas. (Gruber, 1993).

Aunque no existe una ontología especifica de operaciones en el ciberespacio como ya lo existe en otros ámbitos de operaciones militares, si existe algunos elementos desde los cuales partir:

— Respecto al ciberespacio:

  - El modelo de datos CYBERDEM[59] estandarizado de SISO[60] que tiene como objetivo facilitar el intercambio de información del ciberespacio entre distintos sistemas, en especial, en contextos de simulación, entrenamiento, análisis y operaciones militares o de ciberdefensa (Simulation Interoperability Standards Organization. 2014).
  - El estándar abierto OASIS TOSCA[61] desarrollado por el consorcio OASIS[62] que permite definir, desplegar y gestionar aplicaciones y servicios en entornos de computación en la nube de forma portátil, automatizada e interoperable (Kirvan y Bigelow, 2023).

— Respecto a la Misión:

  - La ontología C2SIM[63] es una estructura conceptual formalizada que sirve para facilitar la interoperabilidad entre sistemas

[58] Define de forma estructurada los elementos clave (objetos), sus características (atributos) y las relaciones entre ellos.
[59] CYBERDEM son las siglas que se corresponden con: «Cyber Data Exchange Model».
[60] SISO son las siglas que se corresponden con: «Simulation Interoperability Standards Organization».
[61] OASIS TOSCA siglas que se corresponden con: «Topology and Orchestration Specification for Cloud Applications».
[62] OASIS son las siglas que se corresponden con: «Organization for the Advancement of Structured Information Standards».
[63] C2SIM son las siglas que se corresponden con: «Command and Control – Simulation Interoperation Ontology».

de mando y control (C2) y sistemas de simulación, sobre todo, en contextos militares o de defensa. La ontología C2SIM es un modelo formal que define los conceptos, relaciones y estructuras necesarias para que los sistemas C2 y SIM puedan intercambiar información de forma precisa y sin ambigüedades. Está basada en estándares abiertos y es promovida por organismos como la OTAN, SISO (NATO Science and Technology Organization, 2024).

— Respecto a la amenaza:

- MISP (Multinational Intelligence Sharing Platform), dispone de una pequeña ontología que puede servir de punto de partida para estructurar la información sobre ciberamenazas. Sin embargo, esta ontología necesita ser ampliada y enriquecida, tanto en términos de atributos como de objetos, para cubrir de forma adecuada las necesidades de modelado de inteligencia de ciberamenazas en todos los niveles de la guerra, desde el técnico hasta el estratégico.
- Las «Matrices MITRE ATT&CK», que permiten representar las tácticas, técnicas y procedimientos (TTP) utilizados por los actores de amenazas.
- El «Modelo de Diamante» de análisis de incidentes de seguridad y ciberataques.

6.3 Aplicación de Inteligencia Artificial (IA)

La IA (DL[64] y ML[65]) desempeñará un papel clave en los procesos de análisis de datos e información. Gracias al diseño del sistema y a los módulos especializados de IA, el SCOMCE proporcionará una capacidad avanzada de procesamiento inteligente de datos, de modo que integrará capacidades de análisis, correlación y automatización que faciliten (Kirkpatrick,2024):

— Automatización de tareas[66]: el sistema también incorporará funcionalidades de inteligencia artificial orientadas a automatizar tareas repetitivas o de alto volumen, como:

[64] DL es una sigla que se corresponde con: «Deep Learning», Inteligencia Artificial basada en redes neuronales.

[65] ML es una sigla que se corresponde con: «Machine learning» o aprendizaje automático. Inteligencia artificial basada, principalmente, en estudios de análisis estadísticos de regresión.

[66] Este tipo de capacidades de automatización de actividades repetitivas y rutinarias podrán ser llevadas a cabo por agentes de IA, que permitirán reducir el personal necesario para este tipo de actividades rutinarias y que será esencial para poder reducir el tamaño de los Cuarteles Generales y, por lo tanto, su huella táctica, esencial en entornos en lo que las capacidades de detección del adversario por medios satélites, etc. son muy potentes.

- Búsqueda y extracción automática de información o datos desde un repositorio de documentos no estructurados, incluso se señala en qué documento y párrafo se encuentran las respuestas a la búsqueda.
- Generación de borradores de informes, productos de inteligencia y análisis y resúmenes, lo que agiliza el trabajo de documentación.
- Transcripción y análisis de reuniones, que incluye la identificación y extracción de ideas clave y elementos relevantes.
- Priorización inteligente de correos y tareas, lo que ayuda a enfocar los esfuerzos en lo más urgente y relevante. Contestar de forma automática correos rutinarios.
- Organizar y coordinar tareas y reuniones.
- Automatizar flujos de trabajo.
- Revisión gramatical, traducciones, mejoras de estilo, etc.

— Capacidades analíticas avanzadas:

- Correlar información compleja entre múltiples tipos de datos y objetos y detectar conexiones ocultas entre incidentes, comportamientos y entidades.
- Detectar patrones tanto en el comportamiento del sistema como en el de posibles actores de amenazas.
- Detectar anomalías, identificar comportamientos inusuales a partir del modelo habitual del sistema.
- Modelar actores y comportamientos, lo que representa grupos de amenazas en forma de vectores que representen el comportamiento de grupos de amenazas específicos
- Establecer atribuciones técnicas y tácticas, así como comparar el perfil de un incidente con el de actores conocidos para estimar la probabilidad de su autoría.
- Analizar vulnerabilidades históricas, lo que genera mapas de calor que muestran cuáles han sido más explotadas por diferentes tipos de amenazas.
- Reconstruir líneas de tiempo precisas de los eventos, para facilitar la comprensión del desarrollo de los incidentes.
- Relacionar datos actuales con registros históricos, como *logs* o reportes previos, para identificar similitudes o conexiones relevantes.

- Detectar tendencias y evoluciones y comparar comportamientos pasados con los actuales y anticipar movimientos futuros del adversario.
- Asistencia en la investigación de ciberataques, mediante consultas directas a los datos mediante IA, con preguntas del tipo: ¿qué ocurrió al mismo tiempo que ocurrió tal suceso?, ¿qué vulnerabilidades existían en un activo en tal momento en que se detectó tal evento?
- Clasificar y agrupar (incidentes, *logs*, alertas relacionados), lo que permite investigarlos de manera conjunta y eficiente.
- Reducir falsos positivos, lo que refina las reglas de detección y disminuye la carga de trabajo manual de los analistas.

— Análisis predictivo:

- Mediante técnicas de análisis predictivo, el sistema podrá anticipar acciones futuras del adversario y evaluar riesgos potenciales.

— Sensores de detección avanzados: los sensores basado en inteligencia artificial detectará no por firmas estáticas, ni reglas predefinidas por operadores, sino por patrones comunes:

- En *malware* conocidos: se comparan patrones de *malware* conocidos (modelados de *malwares*). Esto permitirá identificar nuevas variantes de *malware*, aunque el código haya sido modificado parcialmente. En lugar de usar firmas fijas, se identifican patrones comunes.
- En comportamiento de actores: mediante modelado de actores de forma automática por IA se podrá detectar comportamientos en los sistemas que se asemejen a los modelados de un actor. Esto permitirá detectar actividades maliciosas por medio de sensores configurados con reglas configurados por modelados de la amenaza directamente, sin intervención humana.

En conjunto, estas capacidades permitirán a SCOMCE mejorar la eficacia operativa, reducir tiempos de respuesta y aumentar la precisión del análisis y la defensa en el ciberespacio. La combinación de automatización, inteligencia artificial y análisis de datos avanzados convierte a esta herramienta en un pilar esencial para la ciberdefensa moderna.

6.4 Aplicación de técnicas de simulación

Una vez modelados los actores de la amenaza, sus comportamientos y el entorno del Ciberespacio, estos modelos pueden utilizarse para ejecutar simulaciones tácticas y operacionales, que permitan:

— Realizar ejercicios de *wargaming* automatizados.

— Evaluar COA[67] de defensa y reacción ante un ataque simulado.

— Realizar Análisis Operacionales, mediante una cooperación o confrontación exhaustiva de forma automatizada de las potenciales COA propias y adversarias a nivel táctico y técnico, mediante la definición de parámetros que diferencien las diferentes COA a definir de un lado y otro.

6.4.1 Simulación como herramienta estratégica

La simulación es una capacidad clave en el ámbito de la ciberdefensa, ya que permite:

— Recrear ataques sobre infraestructuras reales o virtuales.

— Verificar la efectividad de las defensas implementadas.

— Evaluar cómo responde un sistema frente a distintos tipos de amenazas.

En la actualidad, existen herramientas avanzadas que permiten simular el comportamiento de atacantes reales, conocidas como «Breach and Attack Simulations» (Ciberseguridad.blog, (s. f.).

Estas soluciones replican los métodos y tácticas utilizados por actores maliciosos, lo que permite poner a prueba los sistemas de defensa en un entorno controlado. Sin embargo, la mayoría de estas herramientas están desarrolladas por empresas estadounidenses o israelíes y operan desde la nube. Esto implica que, al utilizar estos servicios, se estaría compartiendo información sensible sobre nuestras vulnerabilidades con entidades extranjeras, lo cual representa un riesgo para la seguridad nacional.

Por esta razón, es fundamental que empresas nacionales desarrollen sus propias soluciones de simulación. La arquitectura de estas herramientas debe ser modular y permitir la creación de agentes específicos que simulen técnicas y tácticas utilizadas por diferentes atacantes. Esto facilita una simulación más precisa y flexible, ya que, en lugar de imitar a un atacante completo, se pueden reproducir secuencias específicas de acciones (*workflows*) que siguen el mismo patrón que utilizaría un atacante real.

Existen dos tipos principales de simulaciones:

— Simulación tipo *Live*: reproduce técnicamente el proceso de un ataque y utiliza herramientas y *software* malicioso (modificado o simulado para que no cause daño). Aunque interactúa con el sistema real

[67] COA son las siglas que se corresponden con «Course of Action» (Línea de acción).

y puede generar cierta resistencia por parte de los proveedores de servicios, estas simulaciones no suelen tener consecuencias negativas reales.

— Simulación tipo TTX (*Tabletop Exercise*): se trata de un ejercicio teórico que analiza un posible ataque con el que se comparan configuraciones, vulnerabilidades y herramientas, sin interactuar directamente con el sistema real. Es una forma más segura y menos invasiva de evaluar la preparación ante amenazas.

7 Conclusiones

El ámbito o dominio del ciberespacio ha dejado de ser un ámbito exclusivamente técnico para convertirse en un escenario estratégico de las operaciones militares. Esta transformación exige una evolución desde la ciberseguridad tradicional —centrada en la protección técnica de sistemas— hacia una ciberdefensa integral, basada en el análisis vulnerabilidades del entorno, dirigida por inteligencia de ciberamenazas y enfocada en el cumplimiento de la misión / operación militar.

Sin embargo, la evolución no es técnica, es doctrinal: pasar de proteger sistemas a anticipar ataques, de reaccionar a decidir antes que el adversario. Esa es la esencia de una verdadera ciberdefensa.

El papel de la Inteligencia de ciberamenazas ha sido clave en esta transición, lo que ha permitido anticiparse al adversario, comprender su comportamiento y preparar defensas proactivas y específicas. No se trata solo de proteger, sino de asegurar la libertad de acción en el ciberespacio y garantizar la continuidad de las operaciones militares frente a actores hostiles cada vez más sofisticados.

El proceso de «operacionalización del Ciberespacio», liderado por el MCCE, representa una respuesta innovadora y necesaria para enfrentar los retos actuales. No basta con defender sistemas, hay que defender la misión, identificar al adversario y preparar al entorno digital para resistir, responder y recuperarse ante cualquier ataque.

La verdadera defensa comienza cuando se protege lo que da sentido a los sistemas: la misión. Blindar solo la infraestructura, sin considerar su impacto operativo, es como fortificar un castillo sin custodiar al rey.

El avance de la ciberdefensa y, en particular, de la inteligencia de ciberamenazas depende directamente de la adopción inteligente de nuevas tecnologías no solo para proteger sistemas o elaborar inteligencia, sino para transformar la forma en que se opera y combate en el ciberespacio.

La implementación de plataformas como PICO y el desarrollo de sistemas más ambiciosos como SCOMCE —apoyados en tecnologías de *datalakes*,

inteligencia artificial y simulación— marcarán un punto de inflexión. Estas herramientas permiten automatizar procesos, modelar amenazas, atribuir incidentes, optimizar recursos y ejecutar operaciones defensivas con una base analítica y predictiva.

Por último, es fundamental consolidar una industria nacional de ciberdefensa, capaz de proporcionar las tecnologías necesarias con plena soberanía, de modo que evite la dependencia de terceros y fortalezca las capacidades estructurales del Estado para operar con eficacia en este dominio decisivo del siglo XXI.

En el siglo XXI, las guerras ya no se libran solo en tierra, mar o aire. Se infiltran en redes, se ejecutan en código y se deciden en servidores. El ciberespacio no es solo un escenario: es el frente más dinámico y menos visible de cualquier conflicto moderno.

Disclaimer

Las opiniones o ideas expresadas en este artículo son responsabilidad exclusiva del autor y no reflejan necesariamente las de la Unión Europea ni de la OTAN ni de las FAS de España ni de la Empresa Telefónica Soluciones de Criptografía (TELCRYP, Grupo Telefónica), ni la Empresa INDRA; y no pueden ser consideradas responsables de la mismas, por lo tanto.

Agradecimiento

Las imágenes referentes a la herramienta PICO han sido cedidas y autorizadas para este artículo por la Empresa Telefónica Soluciones de Criptografía (TELCRYP, Grupo Telefónica).

Las imágenes referentes al proyecto ECYSAP han sido cedidas y autorizadas tanto por la Empresa INDRA como por NATO ACT CyBER.

Bibliografía

Arteaga, F. y Alonso Lecuit, J. A. (2025). El concepto de Ciberdefensa Activa. Real Instituto Elcano. [Consulta: 2025]. Disponible en: https://www.realinstitutoelcano.org/analisis/el-concepto-de-ciberdefensa-activa/ LinkedIn+1Real Instituto Elcano+1

Corletti Estrada, A. (2017). Ciberseguridad (Una Estrategia Informático/ Militar). DarFe. [Consulta: 2025]. Disponible en: http://www.darfe.es

Gruber, T. R. (1993). *A translation approach to portable ontology specifications*. *Knowledge Acquisition*. Knowledge Acquisition. *5*(2), pp. 199-220. DOI: https://doi.org/10.1006/knac.1993.1008

Internet Security Auditors. (2025). Evolución del malware: tendencias y cómo combatirlo. Internet Security Auditors. [Consulta: 2025]. Disponibleen:https://blog.isecauditors.com/evolucion-del-malware-tendencias-y-como-combatirloBlog de Internet Security Auditors

Junta Interamericana de Defensa. (2023). *Guía de ciberdefensa: Orientaciones para el diseño, planeamiento, implantación y desarrollo de una ciberdefensa militar* [en línea]. [Consulta: 2025]. Disponible en: https://jid.org/publicaciones/guia-de-ciberdefensa-orientaciones-para-el-diseno-planeamiento-implantacion-y-desarrollo-de-una-ciberdefensa-militar/

Kirkpatrick, R. G. (2024). The Saint Russ Initiative: AI's Cutting-Edge Tactics for Cyber Safety.

Kirvan, P. y Bigelow, S. J. (2023). TOSCA (Topology and Orchestration Specification for Cloud Applications). TechTarget. [Consulta: 2025] Disponible en: https://www.techtarget.com/searchcloudcomputing/definition/TOSCA-Topology-and-Orchestration-Specification-for-Cloud-Applications

Multinational Capability Development Campaign. (2017). *MCDC 2015–2016: MDCO Planning Guide (Version 1.0)*.

NATO Science and Technology Organization. (2024). *Technical description of C2SIM* (STO-EN-MSG-211-2.3). Disponible en: https://www.sto.nato.int/publications/STO%20Educational%20Notes/STO-EN-MSG-211/EN-MSG-211-2.3.pdf

NATO. (2016). Warsaw Summit Communiqué issued by NATO Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw 8-9 July 2016 [en línea]. [Consulta: 2025]. Disponible en: https://www.nato.int/cps/en/natohq/official_texts_133169.htmNATO+7NATO+7European Sources Online+7

Ramiro, R. (s. f.). Conoce la tecnología «Breach and Attack Simulation» (BAS) y resucita tu estrategia de ciberseguridad. Ciberseguridad. blog. [Consulta: 2025] Disponible en: https://ciberseguridad.blog/conoce-la-tecnologia-breach-and-attack-simulation-bas-y-resucita-tu-estrategia-de-ciberseguridad/

Rodríguez, D. (2023). Ni mar ni tierra ni aire ni espacio: el grupo especial del Ejército español que custodia el quinto dominio. *HuffPost*. [Consulta: 2025]. Disponible en: https://www.huffingtonpost.es/tecnologia/ni-mar-tierra-aire-espacio-grupo-especial-ejercito-espanol-custodia-el-quinto-dominio.html

Seguritecnia. (2023). ¿Qué es la ciberdefensa? [en línea]. Seguritecnia. [Consulta: 2025]. Disponible en: https://www.seguritecnia.es/actualidad/que-es-la-ciberdefensa_20230203.html

Simulation Interoperability Standards Organization (SISO). (2024). *SISO-REF-072-2024: Cyber DEM BONES (Base Objects, Networks, Effects, & Specifications)*. [Consulta: 2025]. Disponible en: https://cdn.ymaws.com/www.sisostandards.org/resource/resmgr/reference_documents_/siso-ref-072-2024.pdf

U.S. Department of the Army. (2009). FM 2-01.3: Intelligence preparation of the battlefield/battlespace. Washington, D.C., Headquarters, Department of the Army.

Winterfeld, S. P. (2002). *Cyber IPB*. Global Information Assurance Certification (GIAC). Disponible en: https://www.giac.org/paper/gsec/1752/cyber-ipb/103147Wikipedia+2GIAC+2GIAC+2.