Desarrollo, implementación y evolución de la capacidad “Cyber Situational Awareness (CySA)” en zona de operaciones

Autor: Pérez García, Ángel

Director/es: Fernández García, Norberto

Contacto: Aperga1@et.mde.es

Cada vez son más numerosas las operaciones de mantenimiento de paz en las que España participa a través del Ministerio de Defensa. La gran mayoría de estas operaciones se realizan en el marco de una coalición internacional (OTAN, UE, etc.), lo cual obliga a trabajar con unos medios CIS interoperables, los cuales nos permitan llevar a cabo las labores de mando y control de las operaciones de manera eficaz.

Son una realidad las herramientas que nos permiten tener un conocimiento profundo de la situación en el campo de batalla, pero aún no se dispone de una herramienta que permita integrar el campo de batalla físico con la amenaza cíber.

En este sentido, se está impulsando desde los gobiernos e instituciones la citada integración, considerándose un requisito fundamental, para poder participar en las operaciones de la coalición, disponer de este servicio.

España participa de manera activa en proyectos que persiguen alcanzar este objetivo, pero todos ellos están focalizados en el nivel estratégico, siendo el nivel táctico el primer eslabón de la cadena y la principal fuente de datos de las herramientas de niveles superiores.

Por todo ello, el presente trabajo pretende dar los primeros pasos en el desarrollo de una herramienta que nos permita disponer de información cíber relevante en el nivel táctico y, por lo tanto, tener una Cyber Situational Awareness (CYSA) adecuada a las misiones en las que el Ministerio de Defensa participa.

Palabras clave: CYSA, Nivel táctico, Operaciones, Awareness, Comandante

---

1. Introducción

La incorporación de España en el siglo XX a distintas alianzas multinacionales, trajo consigo el progreso y la evolución del país en numerosas áreas.

Una de ellas fue sin duda el desarrollo de las Fuerzas Armadas, debido a los estándares que exigía la pertenencia a dichas alianzas.

Estas alianzas, no se llevan a cabo estrictamente en el campo de lo político (estratégico) o lo militar (operacional o táctico), entendiendo "lo militar" como despliegue de fuerzas y reduciéndolo a potencia de fuego y armamento. Hoy en día existe un arma más poderosa que cualquiera de las empleadas en el campo de batalla, es transversal y alcanza a todos los niveles del conflicto, la información. El principal reto y el mayor desafío de una alianza es alcanzar la capacidad de comunicarse, coordinarse y compartir información en el campo de batalla, en tiempo real y con garantías de confidencialidad, integridad y disponibilidad.

Alcanzar la interoperabilidad entre los medios de combate de cada uno de los países que la componen, es uno de los planes más ambiciosos que la OTAN está llevando a cabo en la actualidad, en cuyo desarrollo está invirtiendo miles de millones de euros. Una parte muy importante de este presupuesto, lo está destinando a la interoperabilidad entre sistemas de Mando y Control.

El programa FMN (Federated Mission Network) [1] es un referente en este campo. En él, países de la OTAN y países amigos no pertenecientes a OTAN, pero con relaciones militares frecuentes, llevan trabajando desde hace más de 10 años para alcanzar la interoperabilidad en los sistemas de mando y control que se han de desplegar en Zona de Operaciones (ZO).

El programa FMN, por medio de la implementación de espirales sucesivas, quiere alcanzar la interoperabilidad total entre los sistema de mando y control aliados, y ser capaces de desplegar, en un tiempo muy reducido, los sistemas de cada país participante en la operación y operar como un solo sistema compartiendo los servicios que se determinen para cada operación como se puede observar en la Figura 1, la cual refleja el horizonte 2030 de la OTAN.

El concepto de espirales sucesivas consiste en una evolución progresiva tanto de los servicios que ofrece el sistema de mando y control, como de la interoperabilidad entre los miembros de FMN, con esto, conseguimos que la transición sea paulatina y que nadie se quede atrás en el diseño de sus sistemas.

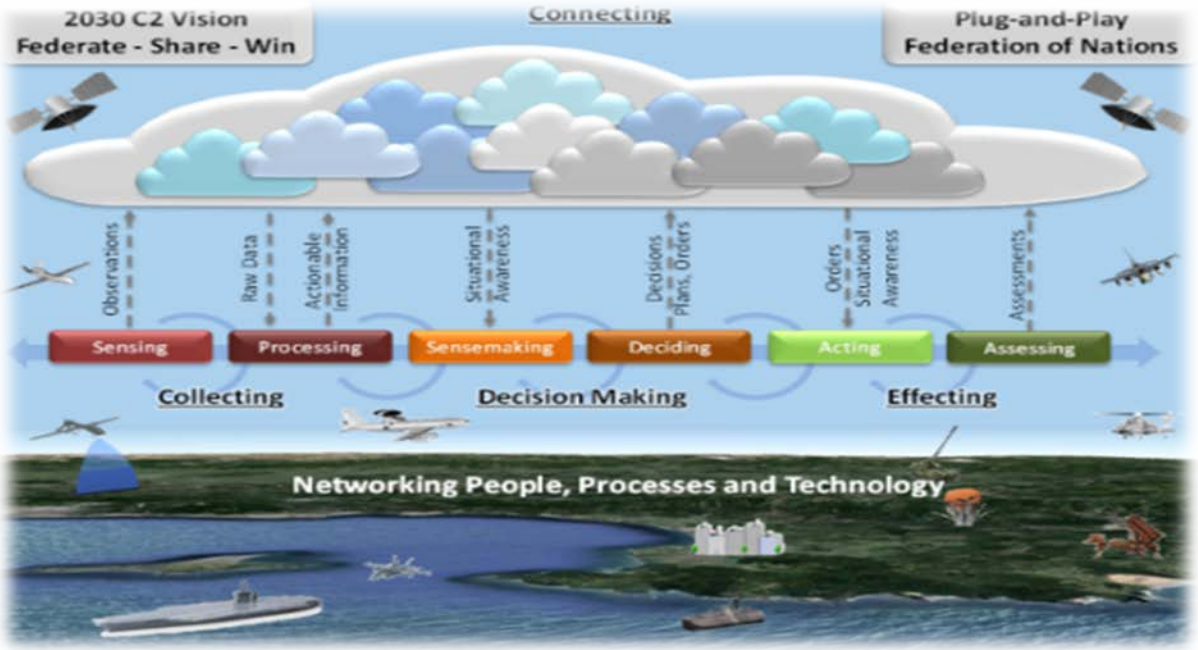

Figura 1. Visión de la OTAN Mando y Control 2030 (Tomada de [2])

Uno de los servicios objeto de estudio en el programa FMN, el cual ha de ser implementado por cada uno de los países miembros y aliados, es el servicio de Cyber Situational Awareness (CYSA), es decir, el conocimiento de la situación desde el punto de vista del ciberespacio.

Cyber Situational Awareness (CYSA) es, a día de hoy, una idea por desarrollar, existen numerosos estudios y aproximaciones al problema [3] y se están llevando a cabo programas encaminados a desarrollar esta capacidad como los de la European Defence Agency (EDA) [4] y la OTAN en el marco de FMN [1], pero aún no hay ninguno que haya llegado a concretarse y no se espera en el corto plazo.

En este documento se pretende llegar a una aproximación en detalle de cómo recoger en el nivel táctico, los datos necesarios de los distintos sistema de mando y control que nos permitan, tras ser tratados adecuadamente, presentar al Comandante la situación del ciberespacio que afecta o puede afectar a las operaciones en curso o venideras.

2. Desarrollo

La CYSA, de manera general, es el conocimiento de la situación relativa a todo aquello que tiene que ver con el ciberespacio y que puede afectar o influir en nuestras operaciones. Es la evolución natural de la Situational Awareness, tan ampliamente extendida en las operaciones militares y que actualmente no se entiende sin su componente cíber.

La CYSA nos ha de permitir integrar y conocer, en todos los niveles de planeamiento, la amenaza cíber y nuestras capacidades en este ámbito.

Para entender mejor el concepto, no debemos olvidar que la CYSA se nutre de fuentes de información de muy distinta índole, como son las herramientas de ciberdefensa, de ciberinteligencia, fuentes abiertas (redes sociales, deep web, etc.), acciones ofensivas de reconocimiento, etc.

Las fuentes de información más relevantes para la elaboración de la CYSA las podemos agrupar en cuatro grupos principales: activos, vulnerabilidades, amenazas e incidentes y medidas de ciberdefensa.

2.1 CYSA en el nivel táctico

La CYSA se puede definir como la comprensión de la situación en el ámbito del ciberespacio que el Comandante alcanza y en la que fundamenta la toma de decisiones.

No se debe perder de vista que la situación es única y no puede ser subjetiva, por lo que la información que la describe debe ser objetiva.

Cada Comandante debe adquirir “su particular” CYSA, para lo cual es necesario que su órgano auxiliar le presente la información con el grado de detalle necesario, atendiendo al ciclo de decisión (Ver figura 2), en el cual influye significativamente el tiempo disponible, y a la misión de cada organización operativa.

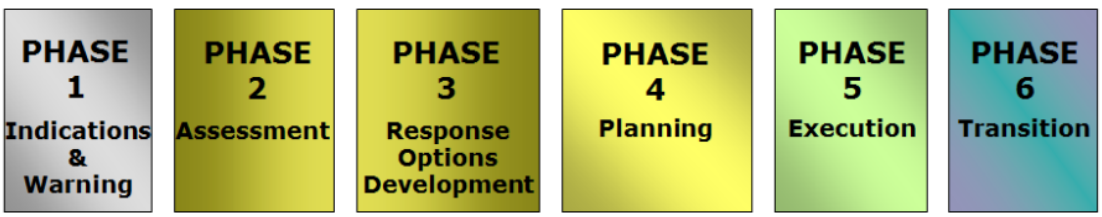

Figura 2. Ciclo de toma de decisión (Tomada de [5])

2.2 Componentes de CYSA en el nivel táctico

En el ciberespacio se conducen acciones ofensivas, defensivas y, además, de obtención de información. Para favorecer la comprensión de la realidad, se propone descomponer la situación en el ciberespacio en componentes que ayuden a su estudio y comprensión.

1) Systems Awareness (SA)
   Este aspecto comprende el conocimiento de los sistemas de interés para el Comandante, incluyendo las capas lógica, ligada a la identificación de los elementos de red, el control de la configuración y los comportamientos anómalos, la física, ligada al conocimiento sobre la ubicación física de los componentes tangibles del ciberespacio, y la humana, ligada al conocimiento sobre el personal que tiene acceso a los sistemas.
2) Enemy Awareness (EA)
   Este aspecto estudia el riesgo que supone el enemigo para los sistemas propios o el CKT (Terreno clave cíber) de interés para el enemigo, así como las oportunidades de las acciones ofensivas propias contra los sistemas o el CKT en poder del enemigo.
3) Mission Awareness (MA)
   Este aspecto estudia los incidentes de seguridad, las fuerzas de ciberdefensa disponibles, los ataques recibidos, las campañas, genéricas o dirigidas, contra la fuerza desplegada, conjugando la situación de los sistemas y del enemigo para valorar el impacto potencial o real que las acciones en el ciberespacio, propias o enemigas, defensivas u ofensivas puedan tener en la misión.

2.3 Presentación de la CYSA

Debido al dinamismo del ciberespacio, para lograr una adecuada presentación es necesario disponer de información actualizada en tiempo casi real. La obtención de la información debe realizarse mediante procesos automatizados o semi-automatizados que la transfieran a una base de datos única.

Una vez la información ha sido obtenida es necesario su tratamiento y presentación al Comandante[1], ya sea el de la operación o jefe de una unidad CIS o cíber. Como ya se ha mencionado anteriormente, cada escalón de mando tiene un tempo en la operación, por lo que es necesario que la presentación de la CYSA se pueda personalizar. De esta forma se evitará tanto la saturación como la escasez de la información necesaria para la adecuada toma de decisiones.

Los responsables cíber (usualmente la célula cíber de un Puesto de Mando) de cada escalón de mando son, habitualmente, los encargados de preparar la presentación de la información que debe conocer y entender su Comandante. Las células cíber de los escalones superiores aportarán la información obtenida por sus propios medios y que pueda ser relevante para la toma de decisiones del escalón o escalones subordinados.

[1] La presentación debe ser adecuada al Comandante como responsable de la toma de decisiones y también a su órgano auxiliar de mando, habitualmente su célula de conducción de las operaciones, donde se ejerce el “control” de las decisiones del Comandante.

3. Prototipo

Desde un punto de vista operativo, el prototipo debe poder mostrar el estado de Ciberseguridad de los sistemas y redes, y en especial de aquellos que son críticos para la operación.

Ha de mostrar de manera clara y visual los datos de los indicadores, los cuales han de ser seleccionados por los usuarios finales de la herramienta, es decir, el Comandante y el personal que le asesora.

Debe poder, en caso de ciberincidente, definir cuál es el alcance del mismo en la red, y cuál es el impacto en la misión. Es decir, debe poder traducir un ciberincidente (nivel técnico) a un lenguaje operativo, que el Comandante y sus asesores puedan comprender de manera visual, intentando dar respuesta a preguntas como:

- ¿Qué impacto tiene ese ciberincidente en la misión?
- ¿Qué riesgo supone una nueva vulnerabilidad en un servicio de un sistema que se emplea en la operación?

Para ello es necesario poder hacer una trazabilidad de las dependencias entre la misión y cada servicio elemental CIS. Es decir, se debe de partir de la misión, e ir desgranando de ella:

- Cuáles son los objetivos de la misión.
- Qué información es necesaria para la misión.
- Cuáles son los sistemas/servicios fundamentales para cada operación.
- Dentro de esos sistemas/servicios, qué subsistemas/subservicios existen y cuáles son esenciales, y así sucesivamente hasta llegar a los servicios más básicos.
- Qué infraestructura (hardware) necesitan dichos servicios/sistemas.
- Que software está desplegado en dichos equipos.

3.1 Modelo de dependencias

En el modelo de dependencias de la figura 3 podemos observar las relaciones entre los distintos elementos. La misión se verá impactada por los elementos de capas inferiores en dos sentidos:

Por un lado, existe una ponderación de las relaciones de dependencia entre la misión y los objetivos, informaciones y servicios/sistemas (“% dependencia” en la imagen), de modo que, por ejemplo, la misión puede verse más impactada por la consecución de un objetivo que de otro, o una información de un servicio/sistema u otro.

Por otro lado, cada elemento del diagrama de dependencias lleva asociado una serie de atributos o características, distintas para cada una de las capas, cuyo valor impactará en la misión. Por ejemplo, la capa de “Software” lleva asociados los atributos “Vulnerabilidad (técnica)” y “Ciclo de vida”. El valor que tomen estos atributos provocará mayor o menor impacto en la misión. Si el software es vulnerable, este valor irá ascendiendo en el diagrama de dependencias hasta impactar o repercutir en el valor de la probabilidad de éxito de la misión.

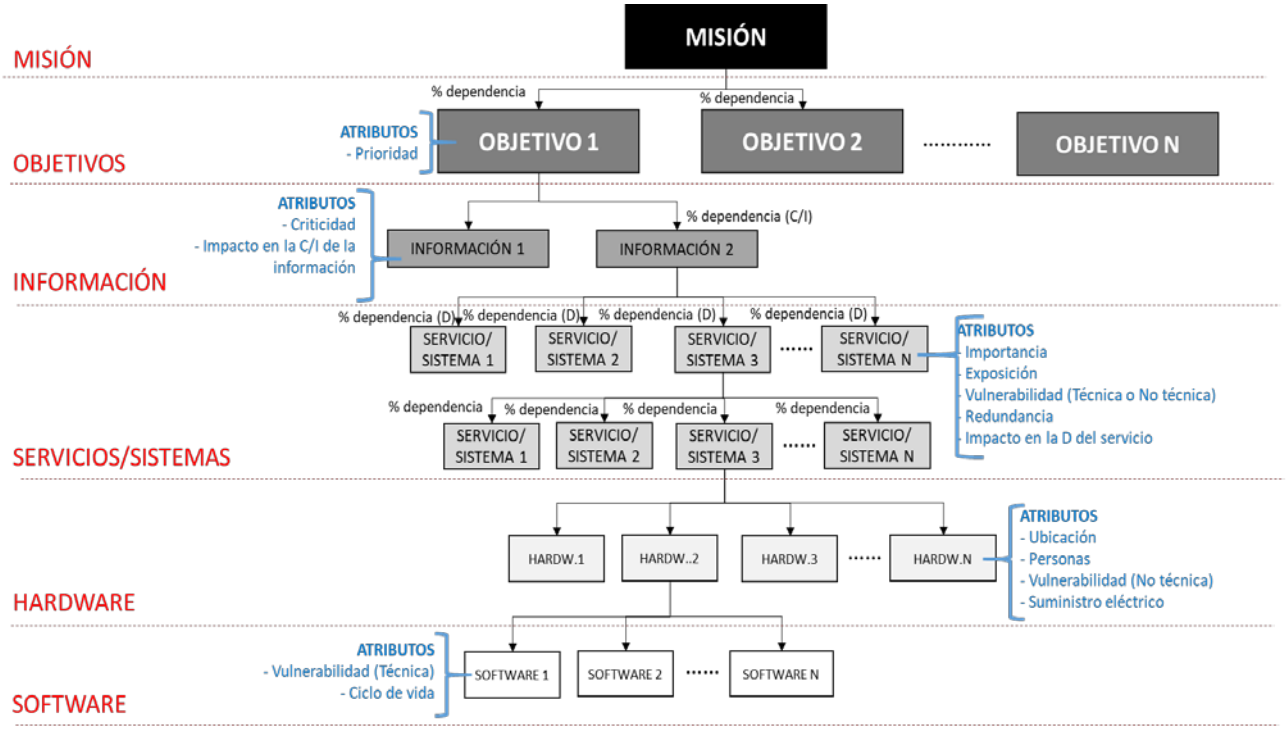

Figura 3. Modelo de dependencias (Elaboración propia)

4. Conclusiones

La necesidad de conocer el entorno que le rodea es fundamental para el Comandante de una fuerza militar desplegada en un ambiente hostil a la hora de tomar decisiones.

Tradicionalmente los esfuerzos se han orientado a proporcionar información de las tres dimensiones clásicas: tierra, mar y aire, incluyéndose en los últimos tiempos el espacio.

Pero la realidad actual es muy diferente, la entrada de una nueva dimensión, como es el componente cíber, ha cambiado la manera de enfrentarse al enemigo.

Para que la adaptación a este nuevo componente sea rápida y ágil, se ha de considerar como uno más de los 4 tradicionales, y se le ha de incluir en el proceso de toma de decisión.

Los proyectos iniciados por los distintos organismos para integrar la CYSA en los procesos de toma de decisiones o en las representaciones gráficas como la NATO Common Operational Picture (NCOP), no son útiles en el nivel táctico, ya que los datos que estos proyectos ofrecen, son de alto nivel y no aportan valor al Comandante a la hora de tomar decisiones, por lo que es necesario llevar a cabo un desarrollo, más sencillo, que englobe y satisfaga las necesidades del nivel táctico.

En el nivel táctico la integración ha de entrar en detalle en los aspectos más importantes en función de la misión, lo cual obliga a que sea una herramienta sencilla y sobre todo muy flexible para adaptarse a la gran variedad de misiones que han de afrontar las pequeñas unidades.

La automatización de los procesos de obtención de información y una representación gráfica simple e integrable con la maniobra (ver figura 4), serán los pilares del éxito del futuro desarrollo, cuyas ventajas a la hora de la planificación de las operaciones es más que evidente.

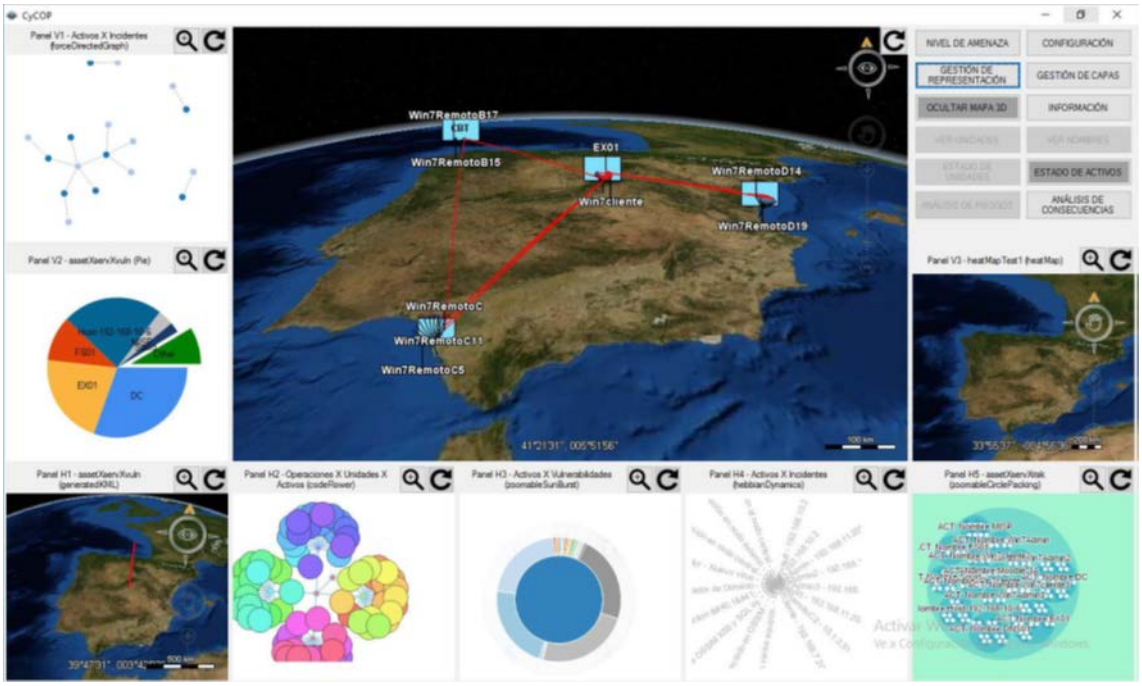

Figura 4.Prototipo Universidad Politécnica de Valencia (Tomada de [5]

Referencias

1. OTAN FMN, «NATO Cooperation Portal,» [En línea]. Available: https://dnbl.ncia.nato.int/FMNPublic/SitePages/Home.aspx. [Último acceso: 13 01 22].NATO CAX FORUM, «NATO Federated Mission Networking Standards,» 2020
2. S. Jajodia, Cyber Situational Awarenes ISBN 978-1-4419-0139-2, Primera ed., Springer, 2010.
3. European Defense Agency (EDA), «Target Architecture & System Requirements for an Enhanced Cyber Situation Awareness (CYSA 2),» 2017.
4. OTAN, «Comprehensive operations planning directive.,» 2013.
5. P. M. Estev, «CYCOP: A cyber hybrid situational awareness and risk analysis visualization tool,» Valencia, 2018.