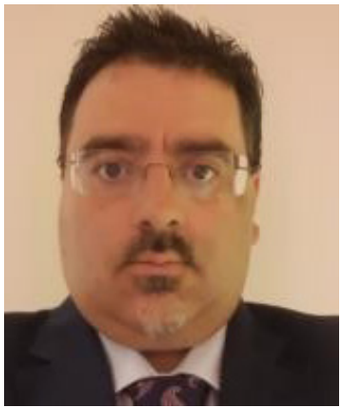
# "MANDO Y CONTROL EN EL CIBERESPACIO: MÁS ALLÁ DE LOS PUROS DATOS TÉCNICOS"

## Command and Control in Cyber Space: Beyond Pure Technical Data

Recibido: 02 / 09 / 2019 Aprobado: 30 / 10 / 2019



Doctor
**José R. Coz Fernández**
España

José Ramón Coz Fernández es Auditor Interno Cyber en el Centro Europeo de Investigación y Tecnología Espacial (ESTEC), en Keplerlaan 1, 2201 AZ Noordwijk. de la Agencia Espacial Europea (ESA). Es Doctor en Economía por la Universidad Complutense de Madrid y Doctor en Ingeniería Informática por la UNED. Además, es Licenciado en Ciencias Físicas por la Universidad de Cantabria, Grado Máster en Economía, Graduado Especialista en Gestión Pública y Máster en Dirección de Tecnologías de la Información por el IDE-CESEM. Posee más de una docena de certificaciones internacionales en Tecnologías de la Información como CISA, CISM, CGEIT, CRISC, PRINCE, MSP, TOGAF o ITIL y varios postgrados en Telecomunicaciones. Tiene más de veinte años de experiencia en el campo de la Auditoría y la Ciberseguridad. Es, además, profesor e investigador en varias instituciones, universidades y escuelas de negocio. Ha realizado multitud de publicaciones científicas y de tecnología, es revisor de varias revistas de ciencia y tecnología internacionales, y es miembro de varias comisiones y asociaciones de auditoría y tecnologías de la información. jose.ramon.coz@esa.int.

Ingeniero
**Vicente J. Pastor Pérez**
España

Vicente José Pastor Pérez es Analista Principal (Compartición de Información Estratégica) y Jefe de la Sección de Soporte de Conciencia Situacional del Centro de Operaciones del Ciberespacio de la OTAN, en 7010 SHAPE, Bélgica, siendo uno de los miembros fundadores del CyOC (Cyberspace Operations Centre).También fue uno de los miembros fundadores de la Capacidad de Respuesta a Incidentes de Seguridad de la OTAN (NCIRC - NATO Computer Incident Response Capability) en la que trabajó durante casi 12 años.Es Ingeniero en Informática por la UNED y posee el Diploma de Estudios Avanzados. Se graduó en el programa de desarrollo de ejecutivos de la OTAN (NATO-wide Executive Development Programme - NEDP) en 2012. Posee diversos diplomas de posgrado entre los que podemos destacar Experto en Seguridad de la Información y Redes de Ordenadores por la UNED, Experto en la Dirección y Gestión de la Información y sus Tecnologías por la Universidad de Alcalá y Experto Profesional en la Gestión de Servicios TI mediante ITIL e ISO 20000 por la UNED. En cuanto a certificaciones, Vicente es, entre otros, Certified Information Systems Security Professional (CISSP), GIAC Certified Forensic Analyst (GCFA) y GIAC Certified Incident-Handler (GCIH). Además, Vicente es Auditor SGSI, Especialista Implantador de SGSI y Experto en Seguridad de la Información por AENOR. Entre otras organizaciones, Vicente es miembro del IEEE, la Computer Society, ISOC y el Colegio Profesional de Ingenieros en Informática de Madrid. En la actualidad se encuentra realizando una tesis doctoral relacionada con sistemas multiagente y su aplicación a la ciberdefensa para mejorar su control centralizado y la conciencia situacional. vpastor3@alumno.uned.es, vicente.pastor@ieee.org.

## RESUMEN

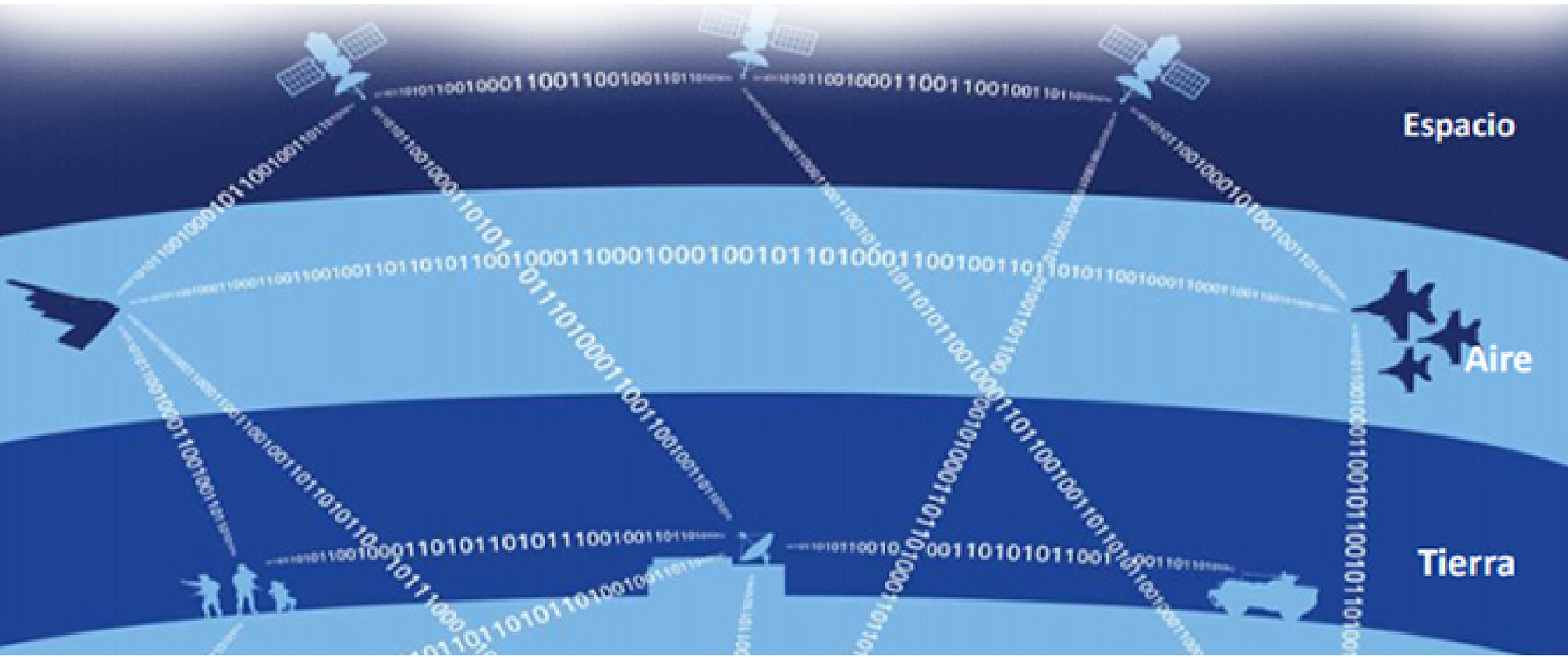
Ríos de tinta han corrido a la hora de describir los requisitos y necesidades para lograr la tan necesitada conciencia situacional en el ciberespacio. Sin el conocimiento adecuado de la situación no es posible conocer las debilidades y las vulnerabilidades presentes y tampoco es posible entender el impacto que sobre las operaciones pueden tener los incidentes accidentales o intencionados. En definitiva, se hace imposible la toma de decisiones a la velocidad adecuada y, por lo tanto, un mando y control adecuado en el ciberespacio. Los autores explican que la ciberseguridad se ha tratado como un silo aislado y, además, se ha estudiado más en profundidad la parte técnica que las dependencias existentes que son las que, en realidad, permiten una toma de decisiones adecuada.

**Palabras clave:**
Ciberespacio, ciberdefensa, conciencia situacional, gestión del riesgo, mando y control.

## ABSTRACT

Rivers of ink have run to describe the requirements and needs to achieve the much-needed situational awareness in cyberspace. Without proper knowledge of the situation, it is not possible to know the actual weaknesses and vulnerabilities and it is also not possible to understand the impact that accidental or intentional incidents may have on operations. Finally, it is impossible to make decisions at the right speed and, therefore, an adequate command and control in cyberspace. The authors explain that cybersecurity has been treated as an isolated silo and, in addition, the technical part has been studied more in depth than the existing dependencies that are the ones that allow for adequate decision making.

**Keywords:**
Cyberspace, cyber defence, situational awareness, risk management, command and control.



## INTRODUCCIÓN

Una vez que el ciberespacio ha sido considerado un dominio más de las operaciones militares, todo lo que hemos hecho hasta ahora en el área de la ciberseguridad y del aseguramiento de la información, se queda muy pequeño para los requisitos que aparecen en este momento. Se trata no sólo de defenderse de posibles ataques técnicos con mayor o menor impacto en las operaciones en los demás dominios, sino también de combatir dentro del ciberespacio y causar efectos en el adversario mediante acciones iniciadas en o realizadas a través del ciberespacio.

Esto hace que si los clásicos en los que se ha movido el mundo cíber, deban ahora desaparecer para entender lo que sucede en el ciberespacio como una parte de un todo mucho mayor. Los responsables de los mandos militares deben entender perfectamente las consecuencias de sus decisiones relacionadas con la parte tecnológica en todas las fases del planeamiento de sus operaciones, algo que ya se hacía hasta el momento. Pero ahora, además, tienen que entender su evolución y el cambio en el valor de los riesgos calculados durante la ejecución de las operaciones, en muchos casos debido a eventos inesperados o descubrimientos sobre las debilidades y vulnerabilidades propias o sobre las capacidades del adversario posteriores a esa fase de planeamiento.

Dos son los retos principales para poder operar en este nuevo entorno. El primero, la velocidad con la que ocurren los cambios, se conocen esos eventos o se descubren nuevas vulnerabilidades o debilidades y la necesidad de conseguir que la ventana de oportunidad del adversario sea lo más pequeña posible. El segundo reto es conseguir crear un conocimiento y, en un paso posterior, un entendimiento del ciberespacio idealmente completo pero que nosotros calificaremos de suficientemente amplio. La complejidad en este dominio creado por el hombre y que cambia a una velocidad nunca vista harán que esta tarea sea muy difícil de abordar y sus objetivos muy duros de alcanzar si no dedicamos los recursos necesarios y si no somos lo suficientemente disciplinados como para seguir unos procesos marcados de antemano.

Una vez conseguido ese entendimiento de la situación, empezando por nuestros propios sistemas y dependencias, pero luego extendido potencialmente a los del adversario, podremos entonces pasar a una siguiente fase, la de proyección de lo entendido hasta el momento para intentar predecir lo que ocurrirá y minimizar los posibles efectos. Es justo después de realizar esa proyección, cuándo estaremos en condiciones de realizar la toma de decisiones necesaria en todos estos casos.

Hasta aquí nos hemos enfocado en lo que llamaremos relaciones verticales que van desde un nivel inferior, el técnico, pasando por el nivel militar (táctico, operativo, estratégico) y llegando al nivel político. Claro que esto no es suficiente si no tenemos en cuenta lo que llamaremos relaciones horizontales, y si dejamos que el ciberespacio como nuevo dominio de las operaciones militares exista desconectado del resto de los dominios cuando la realidad es muy diferente.

Todos los dominios tienen más y más dependencia de los servicios técnicos proporcionados por las telecomunicaciones y los sistemas de información. Por esto, debemos ampliar nuestro modelo para entender esas dependencias y calcular los riesgos y sus variaciones.

La única forma de ejercer un mando y control efectivo, es tener esa visión holística que permita a nuestros comandantes militares entender las consecuencias reales de esos eventos y cambios técnicos que hemos comentado, en términos que les permitan tomar las decisiones adecuadas de acuerdo con la misión. Y es ahora el foco de todo este esfuerzo, el aseguramiento de la misión, la ejecución de acciones militares y también en el ciberespacio.

En el presente artículo, los autores tratan diversos aspectos relacionados con la ciberseguridad, comenzando por elaborar el concepto de conciencia situacional, clave para entender el resto de los procesos; posteriormente, analizando los elementos que son indispensables para su apropiada gestión; a continuación, se analizan las relaciones entre las diferentes partes, y, por último, se exponen las principales conclusiones.

## LOS TRES ELEMENTOS DE LA CONCIENCIA SITUACIONAL: REDES, AMENAZAS Y OPERACIONES

El factor clave que determina la calidad del resultado de la toma de decisiones en cualquier campo es la conciencia situacional. En el ciberespacio, pese a que conceptualmente podamos estar ante un proceso maduro, su implantación no lo es del todo (Coz y Pastor, SIC F13), pues se trata principalmente de ser plenamente conscientes de la situación en la que nos encontramos y de las conse-

cuencias absolutas y relativas de cada una de las opciones frente a nosotros.

En el caso de algunos países y organizaciones internacionales, se opta por un uso holístico que aglutina multitud de capacidades, que incluyen entre otras la monitorización continua, la gestión de los problemas, los eventos y logs, los riesgos, los contenidos, las licencias, las vulnerabilidades y los parches, la protección perimetral, el aseguramiento del software y las auditorias, la gestión de la informática forense, los equipos de gestión de la respuesta y la propia gestión de la seguridad de la información (Coz y Pastor, SIC A13). Todo ello debe estar orientado a un proceso de gestión del conocimiento de los activos de información y las amenazas, y para ello es clave dotar de una compartición adecuada de la información que nos permita el intercambio de los datos y la información necesaria con diversos foros públicos y privados (Coz y Pastor, SIC N14).

Desde el Mando Aliado de Operaciones de la Organización del Tratado del Atlántico Norte (OTAN) se ha desarrollado un marco que permite caracterizar esta conciencia situacional en el ciberespacio a través de la identificación de tres elementos clave para su gestión. Estos elementos, que se pueden observar en la figura siguiente, engloban las amenazas, la situación de las redes y sistemas, y la situación de las misiones, actividades y operaciones (Ali, 2016). A continuación, en los siguientes sub-apartados, expondremos las principales características de cada uno de estos elementos. Por último, mencionaremos algunas iniciativas internacionales para el intercambio de información.

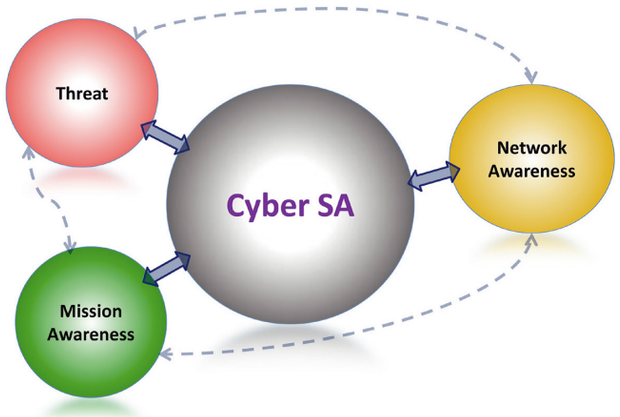



*Figura 1: Marco de Conciencia Situacional del Ciberespacio de la OTAN.*

## LA GESTIÓN DE LAS AMENAZAS EN LA CONCIENCIA SITUACIONAL

En el caso de la gestión de las amenazas, hay que considerar diversos actores que participan, tanto dentro de las estructuras de los Estados, como fuera de ellas, incluyendo las principales fuentes de amenazas como los criminales, los activistas (en ocasiones extremistas), el personal infiltrado y los terroristas. Al hablar de ciberamenazas, normalmente se mencionan los resultados relacionados con capacidades o tácticas tecnológicas para alcanzar un determinado objetivo, pero a nivel estratégico, una de las principales metas es el conocimiento de quién está detrás de esos procedimientos técnicos, qué intentan conseguir y por qué.

Las fuentes que se pueden utilizar para obtener información sobre las potenciales amenazas son múltiples. Nosotros vamos a destacar cuatro de ellas, representadas en la figura dos:

1) Información de fuentes abiertas, tales como informes de prensa, análisis académicos o cualquier otra accesible al público en general, incluyendo la puesta en funcionamiento de herramientas de inteligencia asociadas al análisis de fuentes abiertas tipo OSINT (Open Source Intelligence), bien desarrolladas o parametrizadas ad hoc, en base a las necesidades específicas de la organización, o bien haciendo uso de herramientas o servicios comerciales dispuestas a tal fin.

2) Informes de situación y de amenazas realizados específicamente por la industria, incluyendo herramientas al efecto proporcionadas por las empresas o servicios específicos a medida, en base a las necesidades de la organización. En la mayor parte de los casos, disponer de estos informes requiere un contrato previo para su acceso. Existen multitud de opciones en el mercado en función de las necesidades.

3) Informes clasificados de inteligencia producidos en la propia organización, como pueda ser el caso de organizaciones militares o gubernamentales, que tienen sus propias capacidades para realizar esta tarea, o proporcionados por organizaciones de otros estados o fuentes públicas. En el caso de los informes elaborados por entidades estatales, en la mayor parte de los países existen Centros de Respuesta a Incidentes (CERT) que publican regularmente este tipo de informes. Incluso, en

el caso de Infraestructuras Criticas, existe una legislación, normativas y guías en muchos países y organizaciones, como en la Unión Europea, que abogan por este tipo de intercambio de información (Directiva 2008/114/CE).

4) A través de procesos de intercambio de información entre la propia organización y otros actores. Por ejemplo, en el caso de la OTAN podemos hacer hincapié en la importancia del intercambio de información a nivel militar de cada uno de los Estados miembros de la OTAN, entre sí de forma bilateral o multilateral, o mediante un modelo centralizado en el que se comparte información con la Organización para que la procese y vuelva a compartir el resultado de sus análisis con todos los Estados miembros. Unos modelos similares de compartición de la información existen también a un nivel superior (el nivel político) y a un nivel inferior (el nivel técnico). Como algunos de estos acuerdos podemos destacar la Asociación OTAN-Industria para la Ciberdefensa (NATO-Industry Cyber Partnership – NICP 2019).


*Figura 2: Fuentes de información para la gestión de amenazas.*

## LA SITUACIÓN DE REDES Y SISTEMAS EN LA CONCIENCIA SITUACIONAL

El segundo elemento clave de la conciencia situacional, es la situación de las redes y sistemas. Lo idóneo sería la disposición de un "mapa" de todo el ciberespacio donde pudiéramos consultar los distintos parámetros de interés a nivel técnico para poder, en nuestro modelo, interrelacionar lo observado a este nivel con lo que nos interesa para nuestra misión y con las potenciales amenazas detectadas (Coz y Pastor, SIC M15).

Sin embargo, un conocimiento completo y exhaustivo del ciberespacio es un objetivo que podemos catalogar como inalcanzable. Una forma de aproximar este complejo mapa es ir recopilando toda la información disponible en diferentes "anillos" que representan nuestra distancia a cada uno de los activos (servicios, procesos y los activos de información que soportan los diferentes sistemas que los componen), de acuerdo con nuestro grado de influencia sobre ellos.

En la mayor parte de las organizaciones el "anillo" más cercano es el de los servicios y los sistemas de información que están bajo responsabilidad de la propia organización. Así que siguiendo el aforismo griego de "conócete a ti mismo", se trataría de llevar a cabo un proceso de adquisición del conocimiento de los activos propios, sus interrelaciones, las dependencias a la hora de proporcionar los servicios, procesos y la contribución de estos servicios y procesos a los objetivos globales del negocio. A modo de operación, se trataría del "reconocimiento" del ciberespacio propio organizativo, que sería el terreno más cercano a nosotros.

Por ejemplo, en el caso de la OTAN se deben de tener en cuenta "anillos" que representan los siguientes niveles: redes, sistemas y servicios propios de la Organización, de los Estados miembros, de los Estados Asociados, de las Organizaciones no Gubernamentales, de otras Organizaciones Internacionales, Internet y el total del ciberespacio.

A los adversarios, en principio esperamos encontrarlos únicamente en cualquiera de los dos anillos exteriores, pero la experiencia nos dice que asumir que esto es así está lejos de la realidad y que el adversario en multitud de ocasiones, se encuentra ya dentro de esos perímetros definidos anteriormente. Está claro que estas zonas no son círculos concéntricos, sus límites son difíciles de definir y que incluso hay solapes entre la mismas, pero aun así es una aproximación a la hora de intentar definir las diferentes áreas de responsabilidad.

Dentro del tipo de información que nos interesa conocer relacionado con las redes, sistemas y servicios deberíamos incluir el estado de disponibilidad y rendimiento de los servicios en tiempo real (lo que podríamos llamar "salud de la red"), las vulnerabilidades que sean susceptibles de ser explotadas y su impacto potencial sobre la disponibilidad, confidencialidad e integridad de la información que gestionan nuestros servicios, los eventos, los

incidentes y los ataques, con su impacto asociado, y las posibilidades que tenemos de retorno a la situación normal, la posible duración de la interrupción o el alcance de la acción llevada a cabo por el adversario. Toda esta información debemos obtenerla de las redes, sistemas, procesos y servicios propios, y de las de los demás "anillos" especificados anteriormente en la medida de lo posible.

## EL ESTADO DE LAS MISIONES, ACTIVIDADES Y OPERACIONES EN LA CONCIENCIA SITUACIONAL

El último elemento clave de la conciencia situacional y probablemente el más importante, es el conocimiento en tiempo real de la situación de las misiones, actividades y operaciones que nuestra organización lleva a cabo. Generalmente los servicios de inteligencia se centran en el primer elemento (amenazas) y los servicios técnicos en el segundo elemento (técnico). Sin embargo, este elemento es el que en realidad es más necesario a nivel estratégico, y debería ser el objetivo principal de la conciencia situacional. Se trata de unir, integrar y relacionar todo lo que hemos observado en el ciberespacio con las misiones, operaciones y actividades que estamos realizando y con lo que ocurre en los demás dominios, para tener una visión lo más holística posible de la situación y poder tomar las decisiones más adecuadas en cada momento.

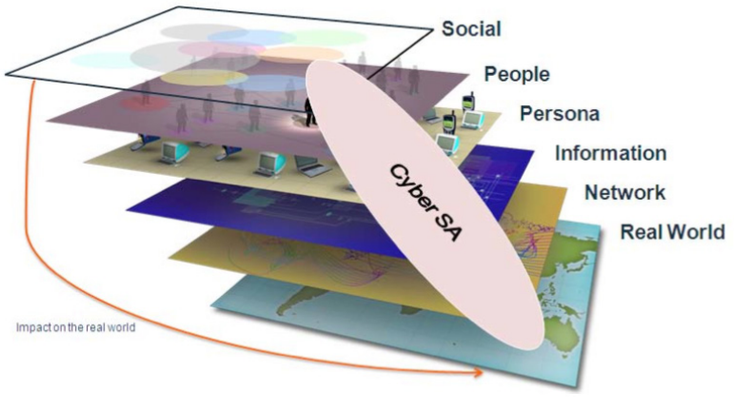



*Figura 3: Lo que ocurre en el mundo virtual tiene impacto en el mundo real.*

A la hora de implementar capacidades que nos permitan soportar esta visión holística, nos encontramos que la mayoría de los sistemas y herramientas disponibles que proporcionan la información de base no son interoperables entre sí, y los fabricantes de este tipo de herramientas y sistemas no proporcionan una vía nada fácil para integrar todos los productos. Es más, a nivel industrial y de competitividad, se considera como una gran desventaja abrir los datos y el código fuente de sus sistemas a la explotación por parte de terceros (Coz y Pastor, SIC F13).

No obstante, podemos destacar que existen multitud de esfuerzos por estandarizar como los realizados por la Corporación Mitre, que estructura las diferentes iniciativas de estandarización en grandes bloques: Registros, Formatos/Lenguajes, Utilización Estandarizada y Procesos Estandarizados. También hay que destacar el Instituto Nacional de Estándares y Tecnología (NIST) del Departamento de Comercio de los EE.UU y sus Publicaciones Especiales, principalmente la serie 800 (SIC 113).

Por otro lado, para poder disponer de dicho conocimiento, es necesario desplegar variados sensores en muy diversos escenarios y algunas veces dispersas, localizaciones que puedan obtener todo lo que sucede en ellas y centralicen posteriormente esa información para su análisis. Ese análisis, que debería realizarse en tiempo real, supondría un acceso muy rápido a grandes volúmenes de datos, lo cual es un gran reto al que las nuevas propuestas de big data, todavía inmaduras, están intentando dar solución. Además, la recolección de los datos relevantes necesarios debería ser obtenida con un grado de fiabilidad alto, en entornos donde su configuración suele ser cambiante de manera continua. Por otro lado, también es bastante complejo el desarrollo de unas métricas que sean las adecuadas y que especifiquen claramente los umbrales a partir de los cuáles se debe o no tomar las diferentes acciones.

## LA CONCIENCIA SITUACIONAL Y ALGUNAS INICIATIVAS INTERNACIONALES

Existen a nivel internacional, diversas iniciativas que tratan de minimizar los riesgos asociados a la gestión de la conciencia situacional, poniendo a disposición información muy útil sobre amenazas y otros aspectos técnicos como el Collaborative ResearchInto Threats - Investigación Colaborativa de las Amenazas (CRIT 2019). Se trata de un repositorio de información sobre malware y amenazas, basado en software abierto y soportado por una herramienta unificada para analistas y expertos en Ciberdefensa.

Por otro lado, tenemos el Collective Intelligence Framework - Marco de Inteligencia Colectiva (CIF 2019), que es un sistema de gestión de inteligencia de ciberamenazas que proporciona diversa información sobre amenazas maliciosas conocidas de diversas fuentes y su utilización para la identificación, detección y mitigación. También destacamos el Framework Mantis (análisis basado en modelos de fuentes de inteligencia de amenazas), (Mantis 2019) que apoya la gestión de la inteligencia cibernética aglutinando diversos estándares tales como: STIX, CYBOX, OPENIOC e IODEF. Finalmente, mencionaremos la Plataforma para la compartición de información sobre malware coordinada por la OTAN (MISP 2019), que reúne a diversos CERT gubernamentales.

Pero además de este tipo de iniciativas, que podemos considerar más de tipo técnico, existen otras a nivel más organizativo o estratégico como los conocidos Centros de Intercambio y Análisis de la Información (ISAC), que nacieron en Estados Unidos como consecuencia de la Directiva Presidencial 63, firmada en mayo de 1998, que reconocía el potencial dañino de los ataques tanto físicos como cibernéticos a las Infraestructuras Críticas de los Estados Unidos, y que dichos ataques podían poner en gran riesgo no sólo a la economía del país, sino también a su potencia militar. Desde entonces los ISAC se han convertido en la base de la gestión del conocimiento para la gestión de Ciberincidentes relacionados con las infraestructuras críticas públicas y privadas, no sólo en Estados Unidos, sino en todo el mundo (Coz y Pastor, SIC M15).

## EL NIVEL TÉCNICO: ¿QUÉ ELEMENTOS SON INDISPENSABLES?

Como hemos comentado, el nivel técnico es en el que más hincapié se ha hecho, obviando en muchos casos el hecho de que los comandantes militares no pueden consumir la información técnica tal cual. El jefe militar necesita una imagen orientada al problema, a su nivel y los informes existentes mantienen la información escondida en extensos campos con datos no estructurados o no está lo suficientemente elaborada para que él/ella pueda entender las implicaciones de lo que está leyendo o está siendo reportado.

Uno de los problemas en el ámbito técnico es que no se dispone de datos continuos como sería de desear para una toma de decisiones casi en tiempo real, sino que únicamente recibimos informes periódicos en los que la información es inherentemente incompleta y confusa. Los flujos de información no contienen todos los datos, o parte de ellos no están contrastados y conllevan ciertas malinterpretaciones que conducen a una toma de decisiones no adecuada.

La comunicación entre partes de la organización o entre organizaciones es inconsistente e incompleta. Los sistemas y los procesos no están adecuadamente diseñados para permitir una compartición efectiva y eficiente de la información lo que hace que se creen burbujas de información que no contribuyen a esa visión global necesaria en la construcción de la conciencia situacional.

Es cierto que tampoco es fácil para los operadores técnicos que han de introducir los datos y la información a bajo nivel y que no entienden las implicaciones de no hacerlo de la manera adecuada. Pero sin una base adecuada es prácticamente imposible construir el conocimiento necesario. Sin información no hay conocimiento.

Si suponemos que partimos de una situación ideal, de cero y que no hay ningún sistema y servicio existente, los datos que son necesarios son los siguientes:

1. **Conocimiento inicial.** ¿Cómo es el diseño del sistema que necesitamos? ¿Para qué lo utilizamos? ¿Cuáles son las dependencias conocidas? Lo que estamos construyendo aquí es nuestra parte preventiva. No tocamos aún nuestra parte reactiva. Este conocimiento inicial incluye:

   a. El diseño inicial de los sistemas y servicios tanto en las fases iniciales de proyecto como en las finales de implementación, es decir, como debería ser el sistema y/o servicio.
   b. Riesgos iniciales calculados, vulnerabilidades y debilidades esperadas, gestión consciente de esos riesgos y riesgos residuales (datos teóricospara cumplir con nuestros propios requisitos de seguridad).
   c. Planes. En este caso nos referimos a la parte de explotación de esos sistemas y servicios técnicos por parte de los usuarios. Si se trata de servicios que utilizamos en el día a día, ¿para qué los usamos? ¿qué dependencia tienen nuestras actividades de esos servicios? ¿Cuál es su resiliencia? Exactamente lo mismo es aplicable a los Planes de Operaciones,

pero con los requisitos elevados que tiene una Operación Militar y teniendo en cuenta el análisis de riesgos de su nivel. En ambos casos, es necesario un conocimiento profundo de las dependencias para entender las consecuencias en cada nivel. Es necesario desarrollar ya en estas fases iniciales un plan de continuidad (de negocio, de las operaciones) con sus correspondientes planes de recuperación de desastres.
d. En esta fase inicial, necesitamos establecer nuestros sistemas de monitorización a nivel técnico, tanto los que nos reportarán sobre la disponibilidad y el rendimiento de los servicios, como los que nos alertarán de posibles incidentes de seguridad. Ambos han de ser diseñados conjuntamente, no por separado.

2. Conocimiento real. A pesar de todo nuestro cuidado en seguir nuestros propios diseños y nuestras propias políticas, la realidad nos dice que las organizaciones son imperfectas en la implementación de éstas. Eso hace forzoso disponer de un conocimiento de la realidad tal y cómo es, no cómo nos gustaría que fuese. En este apartado, estamos interesados en disponer del delta entre cómo debería ser y cómo es en realidad. Estos son los elementos esenciales:

a. Vulnerabilidades y debilidades todavía existentes a pesar de haber sido tenidas en cuenta en la fase inicial. En este punto debemos indefectiblemente realizar las correspondientes auditorías y análisis de vulnerabilidades, así como tomar las medidas correctoras necesarias y proceder a su seguimiento para cerrar el hueco entre lo real y lo planificado.
b. Control y gestión de cambios y configuraciones. Desde que diseñamos nuestras redes, sistemas y servicios, estos se encuentran en continuo cambio por motivos diversos. ¿Tiene la organización un conocimiento claro de estos cambios y de sus posibles implicaciones? El conocimiento de la situación requiere también de esta información.

3. **Conocimiento de los eventos adversos.** Una vez que conocemos la situación, digamos normal, sin influencias externas tenemos que tener en cuenta en el siguiente nivel los eventos adversos. Aquí ya estaríamos en la parte reactiva del proceso. Queremos resaltar tres tipos de estos eventos:

a. Incidentes accidentales, es decir en los que no hay intervención por parte del adversario. Son los típicos incidentes de los que se encarga la gestión de servicios de tecnologías de información. Se trata de problemas inesperados en los equipos u otro tipo de adversidades que influyen en la disponibilidad y el rendimiento de los servicios y que, por lo tanto, pueden tener un impacto notable sobre nuestras actividades.
b. La aparición de nuevas vulnerabilidades o debilidades desconocidas hasta el momento y que, por ello, no fueron tenidas en cuenta en ninguna de las dos fases anteriores. Es necesario un recálculo completo del nivel de riesgo y una toma de decisiones rápida que evite que la ventana de oportunidad sea muy grande y dé más tiempo al adversario para aprovecharla.
c. Los incidentes intencionados, los ataques, en los que es fundamental entender no sólo las implicaciones técnicas sino el objetivo final del adversario uniendo la información con la correspondiente a la amenaza y nuestra propia misión. Quizá uno de los más difíciles de entender ya que tenemos que ser capaces de reconstruir el plan del adversario con unas pocas piezas de información.

La falta de un conocimiento adecuado de la información inicial descrita en el punto 1, hace que no quede más remedio que tomar una actitud reactiva muy ineficiente y en muchos casos, también poco o nada efectiva. Cuando recibimos nueva información, digamos sobre un incidente, si el conocimiento inicial descrito es deficiente, utilizaremos la mayor parte de nuestro tiempo en intentar entender el impacto real de los eventos detectados y posiblemente jamás hallaremos qué es lo que está tratando de hacer globalmente nuestro adversario, al menos no desde la información de un simple evento.

Tenemos que saber que hemos descrito una situación ideal en la que partíamos diseñando todo desde cero. En realidad, ninguno estamos en esta situación, sino que tenemos una infinidad de sistemas y servicios ya existentes. En multitud de casos, tendremos que realizar ingeniería inversa para entender nuestras propias redes, nuestros sistemas y servicios y todas sus dependencias. Y no se trata en absoluto de tarea fácil. La complejidad es muy elevada únicamente teniendo en cuenta el nivel técnico y, si tenemos en cuenta las interdependencias con las actividades correspondientes a las misiones, la complejidad es incluso mucho mayor.

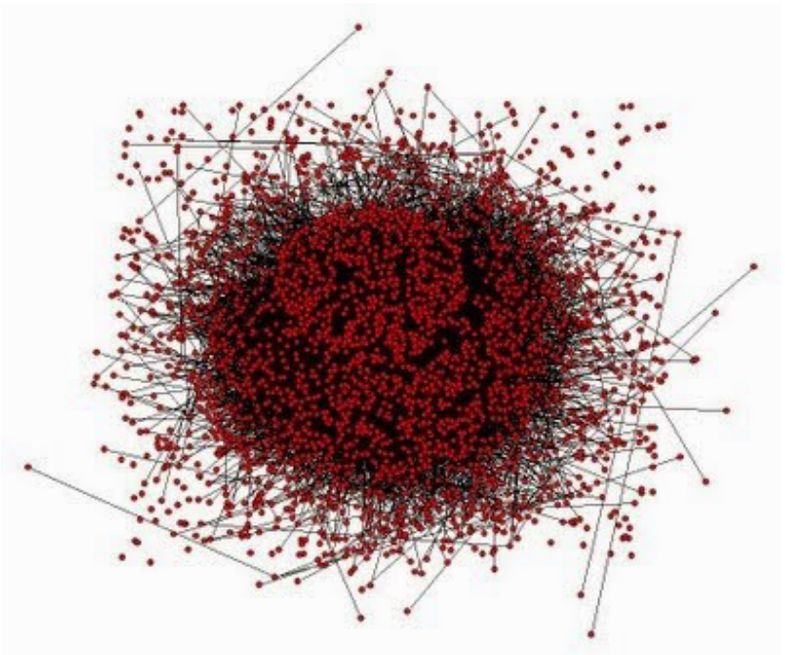


*Figura 4: La complejidad dentro del nivel técnico es muy elevada.*

Otro factor para tener en cuenta es la naturaleza cambiante del ciberespacio. Incluso después de realizar el esfuerzo de esa ingeniería inversa para entender nuestro entorno, eso no basta. Es indispensable mantener esa información actualizada a medida que ocurren esos cambios. Este es uno de los puntos en los que la mayoría de las organizaciones falla. La información desactualizada no sólo pierde su valor con el tiempo, sino que además puede llevarnos a una toma de decisiones deficiente e incluso peligrosa debido a que la información de la que se dispone es errónea y nuestra conciencia situacional es incompleta.

Un aspecto añadido en el que las organizaciones tienen también retos que resolver es en el seguimiento y realimentación de las acciones tomadas tras la aparición de un nuevo evento. Por ejemplo, si se determina que, tras aparecer una determinada nueva vulnerabilidad, nuestro curso de acción consiste en instalar un determinado parche, o cambiar la arquitectura del sistema o reducir la dependencia de la misión del servicio afectado, posteriormente hay que realizar un seguimiento de la compleción de esas acciones, así como recibir la realimentación respecto a la efectividad de la acción que se ha decidido tomar. De otro modo no seríamos capaces de retornar esa información para seguir construyendo el nuevo conocimiento de la situación. Se trata de un proceso continuo, cada nueva decisión y el resultado de esta influyen en una nueva instancia de la conciencia situacional.

Está claro que, sin esta conciencia situacional, que llamaremos de nivel técnico, no es posible una toma de decisiones adecuada. No obstante, el conocimiento a nivel técnico por sí mismo no es suficiente para operar en el ciberespacio. Se hace necesario un conocimiento claro de las interdependencias entre los niveles verticales de nuestra organización y una adecuada comunicación de unos con otros en ambas direcciones de manera que funcionen al unísono y sean percibidos como una sola unidad externamente.

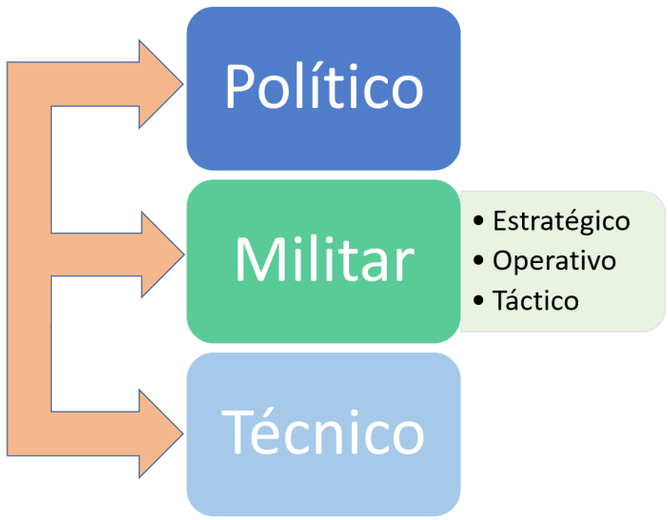



*Figura 5: Relaciones verticales entre niveles para la conciencia situacional en el ciberespacio.*

Cada uno de los equipos en cada uno de esos niveles dispone de un grado de conciencia situacional que ese equipo necesita para realizar su propio trabajo. Esto incluye el hecho de que los miembros de esos equipos que trabajan en el mismo nivel necesitan una conciencia situacional particular (digamos una porción de la conciencia situacional de su nivel) relativa a su cometido. El mismo escenario ocurre en cada uno de los niveles y los equipos que trabajan en un nivel diferente requieren también de su conciencia situacional particular para realizar su trabajo o conseguir su objetivo.

A esto lo llamaremos conciencia situacional de equipo. Por ejemplo, en el nivel técnico, el equipo de detección de intrusiones maneja una porción de la conciencia situacional de nivel técnico diferente a la que maneja el equipo de gestión de vulnerabilidades. Sin embargo, es necesario un conocimiento de la situación técnica único y completo para tomar decisiones adecuadas que afecten a varios equipos. En los otros niveles ocurre de manera similar.

Sin embargo, la toma de decisiones en el ciberespacio, necesita de una conciencia situacional compartida en la que las interdependencias entre los diferentes niveles sean explícitas y exista un conocimiento de la situación que permita una coordinación efectiva de las tareas entre ellos. De lo que se trata es de alcanzar un único entendimiento de la situación por medio de una comunicación efectiva y la comprensión de las interdependencias entre niveles. Es necesario unir esas conciencias situacionales de equipo en una única conciencia situacional global compartida.

## EL CIBERESPACIO COMO DOMINIO DE LAS OPERACIONES MILITARES

La declaración del ciberespacio como dominio de las operaciones militares por parte de varias naciones de manera explícita, abre nuevos retos a la hora de coordinar los diferentes dominios de la guerra.  Y es que, a pesar de que la mayor parte de las representaciones que encontramos, colocan los dominios uno al costado del otro, esta imagen sugiere que no hay interdependencias entre ellos y esto no es en absoluto así.

El problema es aún mayor si tenemos en cuenta la transversalidad del ciberespacio. Este dominio existe en todos los demás y requiere de una coordinación aún mayor que a la que los mandos militares estaban acostumbrados hasta ahora en las operaciones conjuntas. Así mismo, dada la naturaleza global del ciberespacio, se complica la gestión de las operaciones combinadas y se hace necesaria una colaboración con los aliados de manera continua a niveles de detalle antes reservados únicamente a crisis declaradas también en períodos donde no existe ese nivel de crisis.

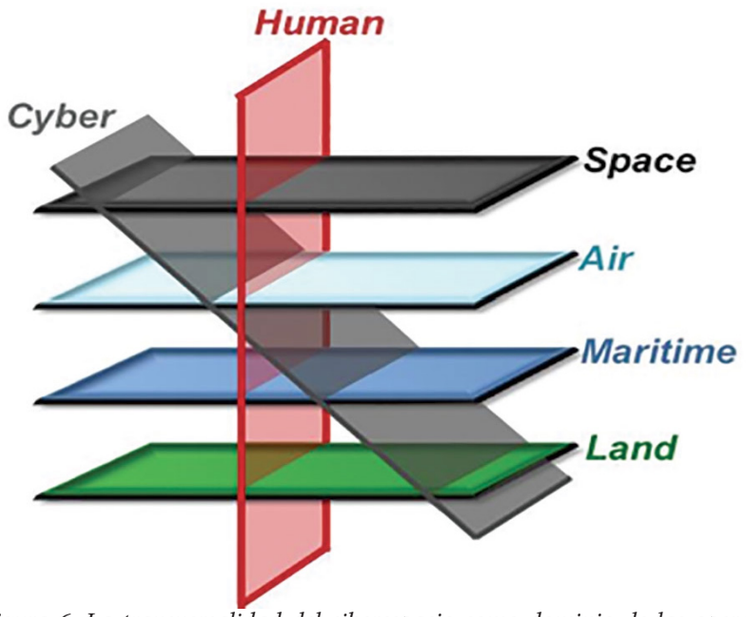



*Figura 6: La transversalidad del ciberespacio como dominio de las operaciones militares.*

Es por lo tanto necesario que la conciencia situacional del ciberespacio sea a la vez alimentada por la información procedente de los demás dominios y además compartida entre todos ellos, para conseguir ese único entendimiento de la situación por el que abogábamos en el apartado anterior cuando hablábamos de las relaciones verticales entre niveles.

En este caso es aún más crítico. Pensemos que la evaluación de la situación, como hemos reiterado, no puede esperar a investigar sobre partes de la información que deben estar disponibles instantáneamente. Surgen por tanto preguntas inter-dominio cuando sucede, por ejemplo, un incidente en el ciberespacio:

- ¿Se trata de un acto intencionado o un evento accidental?
- ¿Cuál es el impacto en mi dominio de operaciones?
- ¿Cuál es el impacto global en la misión?
- ¿Cuál es la situación actual?
- ¿Qué se ha hecho hasta el momento?
- ¿Quién está haciendo qué en este preciso momento? ¿Están las acciones coordinadas entre los dominios?
- ¿Cómo afectan estas acciones a mi dominio en particular? (por ejemplo, si el incidente requiere retirar un determinado

servicio para evitar males mayores)
- ¿Qué es lo que va a suceder a continuación?
- ¿Cuándo puedo esperar la vuelta a la normalidad?

Como vemos de nuevo, se trata de tener claras todas las interdependencias desde un primer momento. Como hemos dicho, la complejidad de los sistemas y servicios, la transversalidad del ciberespacio y la creciente dependencia de estos servicios en cada uno de los dominios hacen que un conocimiento absoluto de la situación sea difícil si no imposible. En todo caso, deberemos tender a que este conocimiento sea lo más completo posible so pena de afectar a la adecuada toma de decisiones.

La clave de todo ello es una conciencia situacional global y compartida que permita conocer tanto la situación de los elementos propios, como los del adversario en tiempo real y para ello necesitamos un conocimiento completo de las interdependencias que, sólo podrá alcanzarse cuando la coordinación y la comunicación tanto en vertical como en horizontal sean eficientes, pero sobre todo efectivas.

## CONCLUSIÓN

Los silos clásicos en los que se ha movido el mundo cíber, deben desaparecer para entender lo que sucede en el ciberespacio como una parte de un todo mucho mayor. Ya no se trata de entender lo que ocurre en el ámbito técnico, sino también de ser capaces de extrapolar esta información y conseguir que los responsables de los mandos militares entiendan perfectamente las consecuencias de sus decisiones, relacionadas con la parte tecnológica tanto durante el planeamiento como en la ejecución de sus operaciones, y todo ello en tiempo real y de manera continua.

El factor clave que determina la calidad del resultado de la toma de decisiones, es la conciencia situacional y alcanzarla en el ciberespacio es una tarea harto complicada. Los mandos militares requieren de una conciencia situacional global y compartida entre niveles de la organización, entre los diferentes dominios operacionales e incluso entre aliados (tanto en operaciones combinadas como fuera de cualquier crisis). De esta manera se posibilita conocer tanto la situación de los elementos propios (y/o aliados), como los del adversario en tiempo real y para ello necesitamos un conocimiento completo de las interdependencias que sólo podrá alcanzarse cuando la coordinación y la comunicación tanto entre niveles verticales como en horizontalinter-dominios sean eficientes y efectivas.

Aún queda mucho camino que recorrer, hasta que se puedan estandarizar estos procesos y se comprenda claramente la necesidad de una conciencia situacional global y compartida. Por lo tanto, los esfuerzos han de concentrarse ahora en crear un modelo que soporte esas interdependencias y dé respuesta a las necesidades descritas.

## REFERENCIAS

Ali, R. (2016). Cyber Situational Awareness for the NATO Alliance. *The Three Swords Magazine,* 30, 72-75.

Collaborative Research into Threats. (2019). Recuperado de https://crits.github.io/

Coz, J. R. y Pastor, V. (2013). La conciencia situacional en la ciberdefensa. *Revista Ciberseguridad, Seguridad de la Información y Privacidad, 103*, 90-92. Recuperado de https://revistasic.es/archivo/images/pdf/sic103-colab.pdf

Coz, J. R. y Pastor, V. (2013). Retos de la conciencia situacional en la ciberdefensa. *Revista Ciberseguridad, Seguridad de la Información y Privacidad, 104,* 88-90. Recuperado de https://www.researchgate.net/profile/Vicente_Pastor_Perez/publication/265413376_Retos_de_la_conciencia_situacional_en_la_Ciberdefensa/links/544052740cf2fd72f99dd5c2/Retos-de-la-conciencia-situacional-en-la-Ciberdefensa.pdf

Coz, J. R. y Pastor, V. (2014). El reto de la compartición de información en la ciberdefensa. *Revista Ciberseguridad, Seguridad de la*

*Información y Privacidad, 112,* 94-98. Recuperado de https://www.academia.edu/9191724/El_reto_de_la_compartici%C3%B3n_de_informaci%C3%B3n_en_la_ciberdefensa

Coz, J. R. y Pastor, V. (2015). ISAC como nexo de unión de las arquitecturas en ciberdefensa. *Revista Ciberseguridad, Seguridad de la Información y Privacidad, 115,* 100-102. Recuperado de https://revistasic.es/archivo/images/pdf/114-colaboracion.pdf

Coz, J. R. y Pastor, V. (2015). STIX: ¿el estándar para la compartición de la información de la Ciberdefensa?. *Revista Ciberseguridad, Seguridad de la Información y Privacidad, 113,* 110-112. Recuperado de https://revistasic.es/archivo/images/pdf/113-colaboracion.pdf

Directiva 2008/114/CE del Consejo. (2008). *Sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección.* Recuperado de https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex:32008L0114

*Malware Information Sharing Platform.* (2018). Recuperado de https://www.ncia.nato.int/Documents/Agency%20publications/Malware%20Information%20Sharing%20Platform%20(MISP).pdf

Mantis. (2019). *Model-based Analysis of Threat Intelligence Sources Framework.* Recuperado de https://django-mantis.readthedocs.io/en/latest/

NATO-Industry Cyber Partnership – NICP. (2019). *Asociación OTAN-Industria para la Ciberdefensa (NATO-IndustryCyberPartnership – NICP 2019).* Fuente NATO Communications and InformationAgency. Recuperado de https://www.ncia.nato.int/Industry/Pages/NATO-Industry-Cyber-Partnership.aspx

The Collective Intelligence Framework. (2019). *Book.* Recuperado de https://github.com/csirtgadgets/massive-octo-spice/wiki/The-CIF-Book