La capacidad de *Ciberdefensa* del Ejército del Aire comienza su andadura

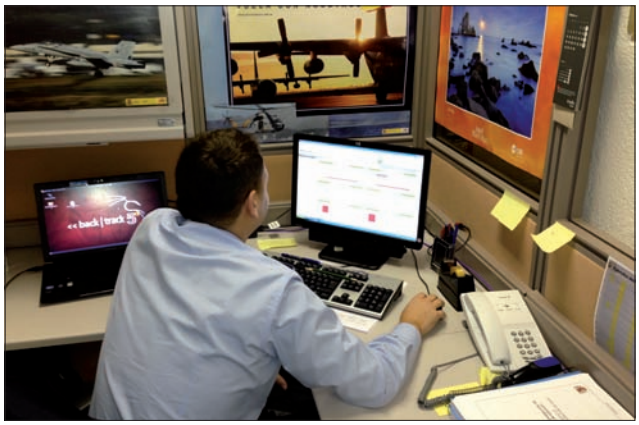
Javier López de Turiso y Sánchez
Teniente Coronel de Aviación

El 15 de febrero el Jefe de Estado Mayor del Ejército del Aire sancionó la 2ª enmienda de la 5ª revisión de la IG 10-2 "Desarrollo de la estructura orgánica del CGEA", por la que se aprobó la creación de la Dirección de Ciberdefensa del Ejército del Aire (DCD), bajo dependencia orgánica y operativa de la Jefatura de Servicios Técnicos y de Sistemas de Información y Telecomunicaciones (JSTCIS), como órgano responsable de gestionar, supervisar, dirigir, planificar, coordinar y ejecutar todas las acciones relativas a la seguridad en Tecnologías de la Información y Comunicación, así como a la Ciberdefensa en el ámbito del Ejército del Aire.
Esta decisión, impulsada por nuestro Jefe de Estado Mayor, es consecuencia de la necesidad del Ejército del Aire de proteger el ciberespacio de su competencia. Nuestro Ejército es uno de los más tecnificados de las Fuerzas Armadas y, por tanto, depende enormemente de los sistemas de información y las telecomunicaciones.

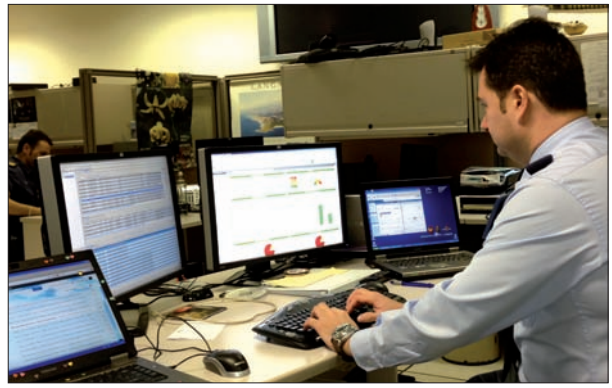
ORÍGENES DE LA NECESIDAD: CIBERESPACIO, EL NUEVO ENTORNO OPERACIONAL

A finales del siglo XX, aparte de los tradicionales entornos operacionales físicos (terrestre, marítimo, aéreo y espacial), el hombre creó un nuevo escenario artificial, desconocido hasta la fecha: el ciberespacio. En la década de los 80, tres hitos significaron el antes y el después en este proceso: el despegue definitivo de Internet, la aparición del ordenador personal (PC) y el surgimiento de los primeros virus informáticos. Esta década dio paso a la era de la información, en la que el desarrollo de la tecnología de los sistemas de información permitió que esta estuviera disponible en cualquier parte del mundo a una velocidad hasta entonces inimaginable. Esto fue posible gracias a la interconexión mundial de redes de ordenadores a las que se le sumaron posteriormente las de comunicaciones. Esta interconexión de redes, formada por multitud de nodos (desde un teléfono móvil, hasta un PC, una impresora en red o un *mainframe*) con sus respectivos enlaces, es lo que vino a denominarse "ciberespacio", que tan solo representa una parte del denominado entorno operacional ciberespacial.

Todo entorno operacional está formado por una parte física (espacios terrestre, marítimo, aéreo, el espacio y el ciberespacio) y unos elementos o factores que conforman los medios de acción propios de cada uno de ellos: medios humanos, materiales o de cualquier



otro tipo. En el caso del entorno operacional ciberespacial la parte física es el ciberespacio[1], mientras que los elementos o factores están formados por personas físicas, identidades virtuales, sistemas operativos, protocolos, información y todo aquello que permita la utilización del ciberespacio para su fin establecido.



En la actualidad, el ciberespacio es el campo de batalla más utilizado al ser el más flexible de todos los entornos. Sirva como ejemplo que en España el número de incidentes críticos ocurridos en 2012 se ha doblado respecto al año anterior.

El Ejército del Aire, como cualquier organización moderna del siglo XXI, también opera en el ciberespacio, el cual es absolutamente vital para el cumplimiento de su misión. El planeamiento y conducción de operaciones, la vigilancia y control aéreo, las comunicaciones, información y órdenes, fluyen en él. El Poder Aéreo requiere superioridad en el ciberespacio. Sin ella, se vería limitado o incluso imposibilitado de actuar.

AMENAZAS Y RIESGOS EN EL CIBERESPACIO

El nuevo entorno operacional comparte características con sus homólogos físicos, pero también tiene otras únicas y exclusivas que le alzan a la categoría de entorno operacional independiente:

- Es el único que engloba a todos los demás; el más flexible; llega a todos los sitios.
- Evoluciona a mucha mayor velocidad que sus homólogos físicos.
- Sus armas no son cinéticas; son baratas, muy sostenibles y de un gran rendimiento.
- Sus ataques presentan mucha mayor velocidad, alcance y potencia, al igual que la difusión de sus efectos.
- Le proporciona al atacante ubicuidad, anonimato (dificulta la atribución de la autoría) y seguridad.
- Se ha convertido en la primera línea de batalla de los actuales conflictos.
- Extiende la zona de combate hasta el corazón de la nación.

Sin embargo, la característica diferenciadora por excelencia es que se trata de un entorno artificial, creado por el hombre. Esta característica hace que el ciberespacio presente imperfecciones o errores (vulnerabilidades; ver Revista Aeronáutica, octubre 2012) que están siendo explotados activamente por diferentes actores con el fin de robar información, alterarla o, sencillamente, inhabilitar medios para evitar que nos proporcionen el servicio esperado. Estas son las amenazas con las que nos enfrentamos en el ciberespacio.

Las ciberamenazas se convierten en riesgo para nuestros sistemas cuando se pueden materializar produciéndonos un daño.

La verdadera dimensión de este riesgo radica en que los actores que pueden explotar las vulnerabilidades de nuestros sistemas constituyen aproximadamente la tercera parte de la población mundial, y en que el daño que una sola persona puede causar en cualquiera de nuestros sistemas podría llegar a ser grave. Por tanto, la deducción del peligro real es una cuestión de matemáticas: el riesgo de que se materialice una de las amenazas por una sola persona es muy bajo; al multiplicarlo por 2.000 millones, se convierte en alto; si además el impacto que puede producir es muy grave, el riesgo se convierte en extremo.

En cuanto a los actores, cualquier estado, grupo o individuo con intereses que colisionen con los de España puede representar una amenaza en el ciberespacio. Existen países que ya disponen incluso de ciberfuerzas (China, Corea del Norte o Irán), algunas de ellas con más de 10.000 efectivos.

Para cualquier Fuerza Aérea o Servicio y, por supuesto, para el Ejército del Aire, determinados ciberataques pueden ocasionarle graves consecuencias operativas. Pero además, si se viera afectada de manera reiterada por estos ataques, ello afectaría a su credibilidad nacional e internacional, pues demostraría su incapacidad para enfrentarse a

[1]Entendido, como se ha dicho antes, como el conjunto de nodos y enlaces físicos, ya sean alámbricos o inalámbricos. No obstante, la definición de ciberespacio todavía sigue siendo controvertida: algunos autores lo consideran de una manera integral (parte física + elementos), otros lo dividen en capas, y otros lo consideran virtual (no real).

estas amenazas. Esto podría ocasionar incluso que se le negase su participación en coaliciones y operaciones aliadas o multinacionales.

Puesto que, llevados por diferentes intereses estratégicos, políticos y económicos, estas ciberamenazas han proliferado exponencialmente en los últimos años, la mayoría de los países del mundo están estableciendo políticas y estrategias de ciberdefensa para luchar contra ellas.

SITUACIÓN DE LA CIBERDEFENSA EN NUESTRO ENTORNO

El problema no es exclusivo de España. El ciberespacio comprende a todos los entornos operacionales físicos de todos los países del mundo. Es un problema a nivel mundial. Actualmente, más de 140 países están adoptando capacidades de ciberdefensa para proteger sus sistemas de información y de telecomunicaciones. Y de ellos, al menos 50 están desarrollando capacidades ofensivas.

EE.UU. es, probablemente, el país más puntero en ciberdefensa a nivel mundial. Tiene ya publicada su Estrategia para operar en el Ciberespacio, tiene creado un Ciber Mando Militar (USCYBERCOM) y tiene iniciados programas como el X-Plan de DARPA para el control en tiempo real del campo de batalla cibernético. Para el 2013 tiene prevista una inversión en ciberdefensa de 769 M $.

Gran Bretaña, aparte de tener también publicada su Estrategia de Ciberseguridad, ha destinado a ciberdefensa para los próximos cuatro años 650 M £.

Por otro lado, tanto la OTAN como la UE han demostrado la necesidad de considerar la ciberdefensa como un objetivo prioritario. Entre otras acciones, la OTAN ha publicado su Política de Ciberdefensa y ha invertido decenas de millones de euros en equipamiento, y la Unión Europea ha presupuestado 400 M € para este cometido durante el periodo 2014-2020.

SITUACIÓN DE LA CIBERDEFENSA EN LAS FAS ESPAÑOLAS

En España, la Directiva de Defensa Nacional 2012, la de Política de Defensa 2012 y la de Planeamiento Militar 2012 hacen referencia a la importancia del ciberespacio para España, y remarcan la necesidad de impulsar la seguridad ante las amenazas del ciberespacio. El último de estos documentos incide además en la potenciación de las capacidades conjuntas de ciberdefensa.

Por otro lado, la Estrategia Española de Seguridad (2011), en proceso de revisión por el actual Gobierno, incluye una especial mención a las ciberamenazas. Finalmente, existe un borrador de Estrategia Nacional de Ciberseguridad (2012), que se encuentra pendiente de aprobación, a la espera de que finalice la revisión del anterior documento.

En el ámbito militar, el JEMAD ha diseñado el proceso para la obtención de una capacidad de ciberdefensa militar, recogido en los siguientes documentos:

• Visión del JEMAD de la Ciberdefensa Militar (enero 2011). Documento que orienta la definición, el desarrollo y el empleo de las capacidades militares nacionales (defensa, explotación y respuesta) necesarias para garantizar la eficacia en el uso del ciberespacio en las operaciones militares.

• Concepto del JEMAD de Ciberdefensa Militar (julio 2011). En el que se exponen los principios, objetivos y retos de la ciberdefensa en el ámbito militar, se define la terminología, se realiza una evaluación de la capacidad, se presentan las funciones y responsabilidades en esta área, y se ordena la elaboración de un "Plan de Acción para la obtención de la Capacidad de Ciberdefensa Militar".

• Plan de Acción del JEMAD para la obtención de la Capacidad de Ciberdefensa Militar (julio 2012). Documento en el que se define la organización de la ciberdefensa militar, que se articula en tres niveles: dirección (EMAD), gestión (EMAD y Ejércitos) y ejecución (EMAD y Ejércitos), y el proceso de obtención de la capacidad en tres fases: inicial (capacidad de defensa), intermedia (capacidad de explotación) y final (capacidad de respuesta).

Finalmente, el 26 de febrero se publicó en el BOD la Orden Ministerial de creación del Mando Conjunto de Ciberdefensa, de nivel estratégico e integrado en la cadena operativa de las FAS, bajo la dependencia directa del JEMAD. La O.M. contempla las definiciones, el ámbito de actuación del Mando, su misión, cometidos, mando y dependencia. Otras cuestiones relevantes para el éxito de este Mando (financiación, composición, personal, ubicación, etc.), quedan pendientes de un posterior desarrollo por el JEMAD.

LA CIBERDEFENSA EN EL EJÉRCITO DEL AIRE

Como consecuencia de todo lo visto anteriormente, el Ejército del Aire se enfrentaba a una situación en la que sus sistemas y la información que manejaban eran vulnerables a los riesgos del ciberespacio. Para hacerles frente, la mayoría de nuestros aliados y los

países de nuestro entorno estaban adoptando medidas relacionadas con la ciberdefensa. En España, el EMAD y la Subdirección General TIC de la Dirección de Infraestructura, estaban impulsando acciones y medidas de ciberdefensa a los sistemas conjuntos y corporativos de los que son responsables. Además, el JEMAD, en el Plan de Acción para la obtención de la capacidad de ciberdefensa militar, asignaba responsabilidades a los Ejércitos y Armada sobre sus sistemas específicos, aparte de aquellos otros sobre los que el Ejército del Aire es el único responsable. Ha sido en este contexto en el que el JEMA aprobó la creación de la Dirección de Ciberdefensa del Ejército del Aire.

LA DIRECCIÓN DE CIBERDEFENSA (DCD)

La Dirección de Ciberdefensa es el órgano responsable de llevar a cabo todas las acciones relativas a la seguridad TIC y la ciberdefensa militar en el ámbito del Ejército del Aire (cuadro).

El *Plan de Acción para la obtención de la capacidad de Ciberdefensa Militar* asigna a los Ejércitos el cometido de obtener la capacidad permanente de ciberdefensa, así como, cuando le sean encomendadas, las de explotación y respuesta, de acuerdo con las directrices que determine el JEMAD. La DCD constituye el elemento orgánico específico del nivel de gestión que recoge la estructura de la organización de la Ciberdefensa Militar que figura en el mencionado Plan de Acción del JEMAD (PACDM) y representa el nexo de unión con el Mando Conjunto de la Ciberdefensa de las Fuerzas Armadas. Asimismo, la DCD es el órgano responsable de fomentar, en el ámbito del Ejército del Aire, la cultura de ciberdefensa.

La Jefatura de la Dirección de Ciberdefensa corresponde a un Oficial del Cuerpo General del Ejército del Aire.

ESTRUCTURA ORGÁNICA

La Dirección de Ciberdefensa está constituida por los siguientes elementos orgánicos:

- Secretaría.
- Sección de Seguridad TIC (Tecnología de Información y Comunicaciones).
- Sección de Operaciones de Ciberdefensa.
- CERT-EA.

Funciones

Sección de seguridad TIC (SESTIC)

La Sección de Seguridad TIC asume todas las funciones que anteriormente venía desempeñando la Sección INFOSEC de la Dirección CIS, a la vez que adquiere otras nuevas relacionadas con la ciberdefensa en el E.A. Las principales son:

– Desarrollar las políticas, doctrinas y normativas de seguridad TIC y ciberdefensa en el EA.
– Definir la organización de seguridad TIC y ciberdefensa.
– Promover la incorporación de la capacidad de ciberdefensa en el proceso de Planeamiento Militar.
– Fomentar la cultura de ciberdefensa. Proponer planes de formación y adiestramiento en seguridad TIC y ciberdefensa.
– Asesorar en materia de seguridad TIC y ciberdefensa a las distintas AOS en la elaboración de la documentación de seguridad de sus sistemas.
– Canalizar ante la ADA (Autoridad Delegada de Acreditación) del Ejército del Aire, las acreditaciones de sistemas.
– Dirigir y gestionar la Cuenta Cripto Principal del Ejército del Aire.
– Controlar el inventario y situación del material cripto en el EA.

Sección de operaciones de ciberdefensa (SOC)

La Sección de Operaciones de Ciberdefensa es la responsable de todas las acciones relacionadas con el planeamiento de las capacidades de defensa y cuando se le encomienden, las de explotación y respuesta, en el ámbito del Ejército del Aire. Entre las funciones de la SOC figuran:

– Definir y planificar la capacidad de ciberdefensa militar en los sistemas del Ejército del Aire.
– Promover las acciones necesarias para la adecuación de la ciberdefensa militar de los sistemas específicos del E.A. a las directrices del JEMAD.
– Divulgación de las mejores prácticas y medidas de seguridad TIC preventivas en las redes y sistemas específicos del E.A.
– Análisis y gestión de riesgos de las redes y los sistemas de información del EA.
– Inspecciones de seguridad en las redes y sistemas de información específicos del Ejército del Aire.
– Recabar y recibir inteligencia relacionada con la ciberdefensa.
– Colaborar con los CERT del Ministerio de Defensa (CERT-FAS, COS-DEF, CERT-ET, etc.).

La Sección de Operaciones de Ciberdefensa encuadra como elemento orgánico el Centro de Gestión de Incidentes de Seguridad del Ejército del Aire (CERT-EA).

Centro de Gestión de Incidentes de Seguridad (CERT-EA)

El CERT-EA constituye el elemento orgánico específico del nivel de ejecución (Célula de Defensa) que recoge la estructura de la organización de la Ciberdefensa Militar que figura en el Plan de Acción para la obtención de la capacidad de Ciberdefensa Militar del JEMAD (PACDM).

En las redes y sistemas de información específicos del Ejército del Aire, el CERT-EA será responsable, entre otros, de los siguientes cometidos:

– Realizar análisis de vulnerabilidades.
– Monitorizar y detectar incidentes de seguridad.
– Ejecución de las actividades de explotación y respuesta que, llegado el caso, les sean encomendadas por el EMAD.
– Analizar, evaluar y resolver incidentes de seguridad TIC.
– Actividades de recuperación de la información.
– Análisis forenses posteriores a los incidentes detectados.
– Proponer acciones correctivas que eviten la repetición de incidentes y establecer un sistema de lecciones aprendidas.
– Participar en los ejercicios de ciberdefensa que se le encomienden.

DEPENDENCIA

La Dirección de Ciberdefensa depende orgánica y operativamente del General Jefe de la Jefatura de Servicios Técnicos y de Sistemas de Información y Telecomunicaciones.

PLAN DE IMPLANTACIÓN

Para la implantación de la DCD se ha aprobado un Plan de Trabajo articulado en fases. Tras la superación de la fase inicial, con la modificación de la IG 10-2, las modificaciones iniciales de la plantilla orgánica y la RPM y la designación del Director de Ciberdefensa, se encauzarán las tres si-

guientes, con los objetivos que se describen a continuación:

• Fase 1: definir la política, doctrina y organización de la ciberdefensa en el EA.

• Fase 2: identificar los escenarios y determinar qué hay que defender y contra qué, en el ámbito específico del E.A., con el objetivo de conocer la situación actual del ciberespacio E.A., realizar el análisis de riesgos de nuestras redes y sistemas, y determinar las prioridades de securización.

• Fase 3: determinar cómo se van a defender e implantar progresivamente, según la priorización establecida, las medidas de prevención, monitorización, detección, contención, resolución y recuperación, para así desarrollar las capacidades de análisis, reacción y respuesta.

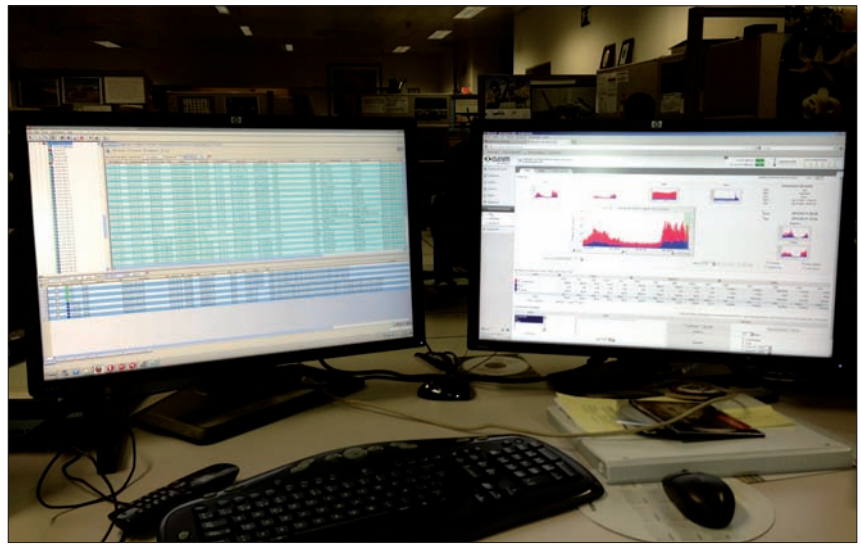
El calendario previsto para las fases 1 y 2 es de unos 12 meses, y para la fase 3, dependerá de la disponibilidad de recursos. Durante ellas se deberá incorporar nuevo personal a la Dirección. Los primeros 7 puestos ya han sido creados y están en proceso de publicación y cobertura; durante la 1ª fase se definirá el resto de la plantilla necesaria, que deberá ser creada y publicada en los próximos meses.

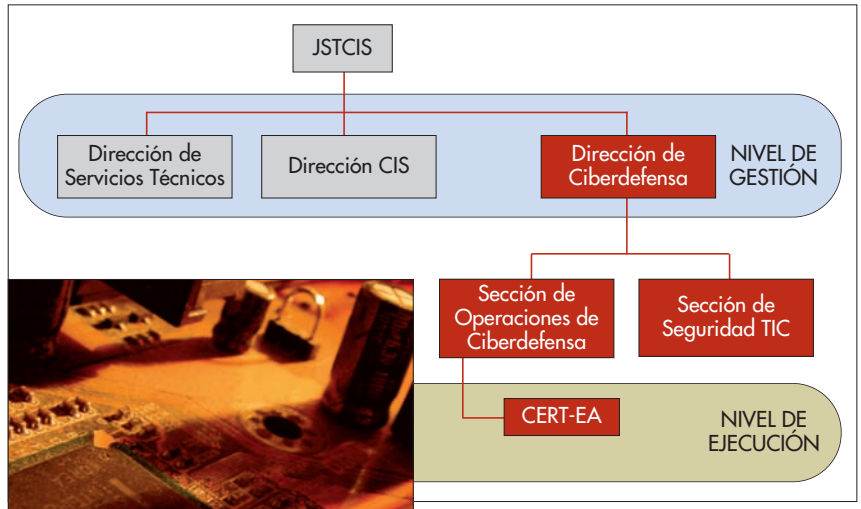
CONCLUSIONES

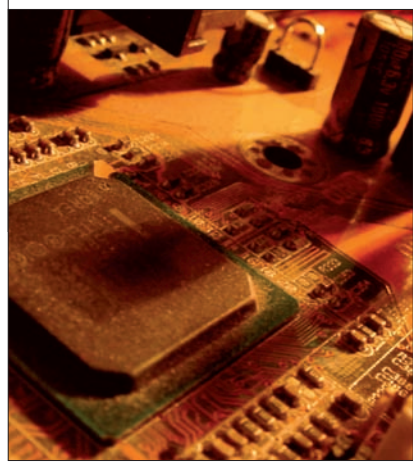
El ciberespacio es el nuevo entorno operacional impuesto por la sociedad de la información, que no solo engloba, sino que llega hasta las mismas raíces de todos los entornos operacionales conocidos, incluido, por supuesto, el aéreo.

Hoy día, la dependencia de la sociedad y, por ende, de las Fuerzas Armadas y del Ejército del Aire, del ciberespacio, es total. Sin su control, el empleo del Poder Aéreo se vería limitado o impedido, y el Ejército del Aire no podría cumplir su misión. Por ello, es prioritario alcanzar la superioridad en el ciberespacio, lo que demanda la creación de una organización de ciberdefensa, la elaboración de una doctrina y la asignación de recursos de personal y material.

El Ejército del Aire ha reconocido esta necesidad y ha demostrado tener la voluntad y determinación para acometerlo. Con la creación de la Dirección de Ciberdefensa, el Ejército del Aire afronta el reto del ciberespacio, muestra su firme determinación para contribuir a la capacidad conjunta, y define la







organización que en el ámbito específico formará parte de la organización de la ciberdefensa militar. La organización y cometidos de la Dirección de Ciberdefensa, así como las responsabilidades que asumirá sobre los sistemas específicos del Ejército del Aire, se ajustan a lo establecido por el JEMAD.

El futuro de la ciberdefensa en el Ejército del Aire debe enfrentarse a más retos, como la consecución de la adecuada coordinación con el Mando Conjunto de la Ciberdefensa y, muy especialmente, la formación de su personal que, para el cometido tan específico a desarrollar, requiere contar con una profunda especialización, dedicación exclusiva y una adecuada permanencia en los destinos.

Nos encontramos ante la misma situación que vivió el nacimiento del Poder Aéreo como poder diferente y diferenciado de los entonces conocidos terrestre y naval, o el nacimiento de las Fuerzas Aéreas y Ejércitos del Aire tras la experiencia de la Primera Guerra Mundial: una situación nueva, que requiere ser comprendida en toda su complejidad para poder ser valorada y, sobre todo, que exige ser analizada con visión de futuro, para así poder tomar las decisiones que permitan dotar al EA de la capacidad que precisa para alcanzar la necesaria superioridad en el ciberespacio y asegurar el empleo del Poder Aéreo con libertad ■