MCCE

El Mando Conjunto del Ciberespacio asegura la libertad de acción de las Fuerzas Armadas en este nuevo entorno operativo

Defensa EN LA ERA DIGITAL

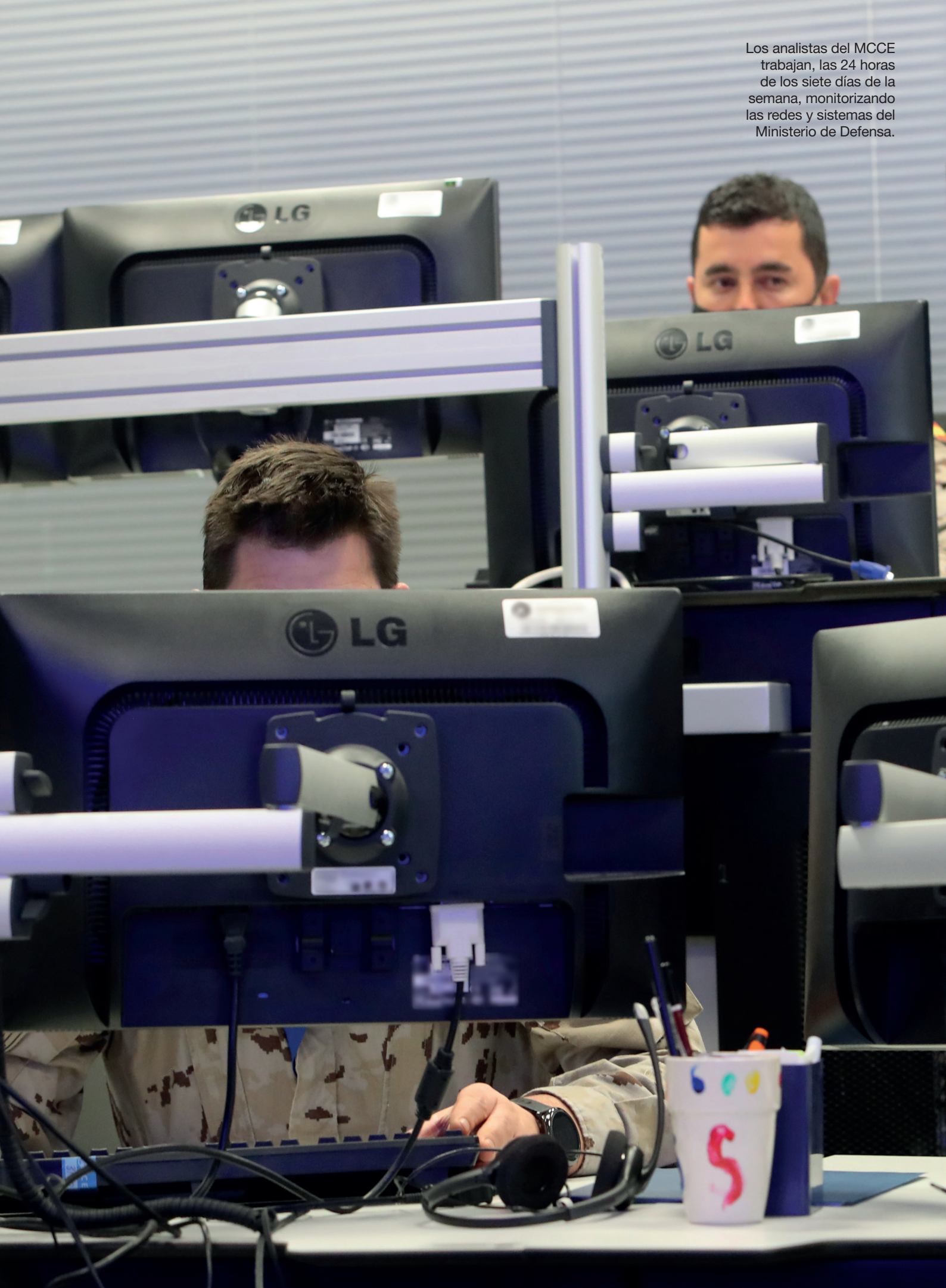
MCCE

LOS ciberataques son silenciosos y, a menudo, imperceptibles. Aprovechan alguna debilidad o vulnerabilidad de los sistemas informáticos para infiltrarse en ellos y afectar a cualquier ciudadano o institución, también a elementos críticos para la Defensa y las operaciones militares. El órgano responsable de asegurar la libertad de acción de las Fuerzas Armadas en este nuevo campo de batalla es el Mando Conjunto del Ciberespacio (MCCE).

Es la unidad más joven de las Fuerzas Armadas. Se constituyó en mayo de 2020 como la culminación de un proceso en el que se fusionaron la Jefatura de Sistemas de Información y Telecomunicaciones de las FAS y el Mando Conjunto de Ciberdefensa. Ahora, además de sus funciones «ciber», se pueden acometer misiones sobre los sistemas de mando y control y también sobre guerra electrónica que antes no tenía atribuidas.

«El Mando está a pleno rendimiento; para ello, se ha organizado creando nuevas jefaturas por áreas de conocimiento», explica el contralmirante Javier Roca, segundo comandante del MCCE. «En el ámbito ciberespacial participamos en las operaciones permanentes, en la *Misión Baluarte* y apoyando las operaciones en el exterior; en el área de mando y control, estamos inmersos en conseguir la capacidad operativa inicial del Sistema de Mando y Control Nacional (SC2N), primera prioridad del jefe de Estado Mayor de la Defensa».

Entre los objetivos más inmediatos del Mando se encuentran también los de aumentar su plantilla y consolidar el futuro Sistema de Combate del Ciberespacio (SCOMCE). «Este sistema —añade el contralmirante Javier Roca— permitirá al conjunto de las Fuerzas Armadas operar en total coordinación y adiestrarse convenientemente para proteger y defender nuestras redes y sistemas en el caso de que sean atacados».



Los analistas del MCCE trabajan, las 24 horas de los siete días de la semana, monitorizando las redes y sistemas del Ministerio de Defensa.

Ejército del Aire

Personal del MCCE ha formado parte del equipo encargado de verificar la integridad de los sistemas de información del destacamento *Paznic*, en Rumanía.

España, que en 2013 fue una de las pioneras en crear un Mando Conjunto de Ciberdefensa, se encuentra actualmente bien posicionada en esta materia, tanto en la OTAN como en la Unión Europea. No obstante, «en un ámbito tan cambiante como este y donde los adversarios avanzan a pasos agigantados, mantenerse es retroceder; algunos analistas ya anticipan que pronto la ciberseguridad será tan importante como la propia electricidad», advierte el contralmirante Roca.

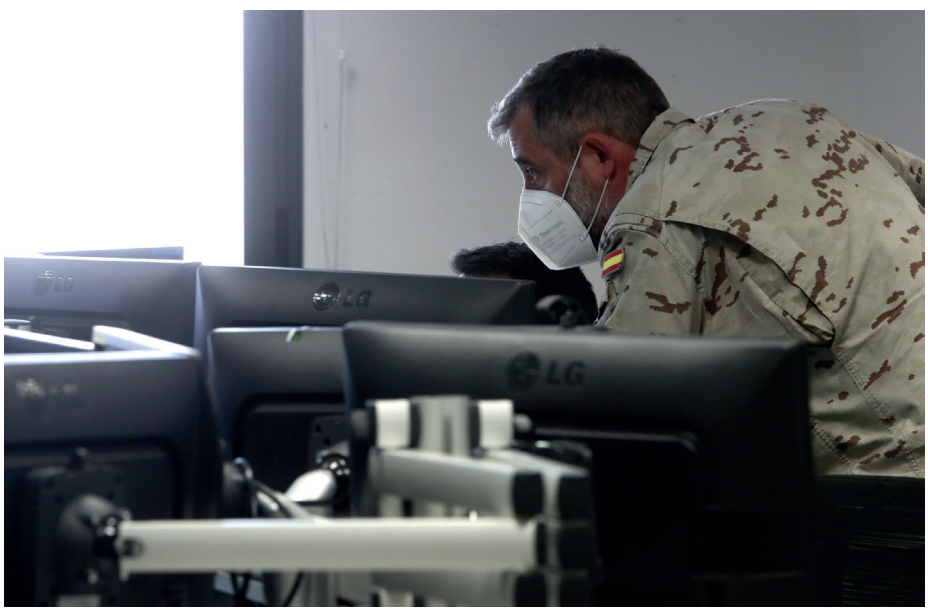
PROTECCIÓN

El primer deber del MCCE es garantizar que las redes y sistemas del Ministerio de Defensa estén seguros. Como indica el capitán de navío Manuel Alvargonzález, jefe del Estado Mayor del Mando, «tenemos que proteger nuestros datos, nuestra información, y mantener nuestras capacidades militares. Y también poder usarlas como una herramienta para asegurar la libertad de acción en el ciberespacio». Todo ello se realiza desde el Centro de Coordinación y Control de Ciberdefensa (C4D) del MCCE, ubicado en un edificio clasificado en la base de Retamares.

El año pasado se formó el primer Mando Componente del Ciberespacio de una operación nacional, la de *Misión Baluarte* contra el coronavirus, bajo el mando del comandante del Mando de Operaciones (MOPS). «Empezamos prácticamente con una hoja en blanco y con mucho trabajo e ilusión —observa el capitán de navío Alvargonzález—. Los resultados han superado nuestras expectativas. Durante todos los días de la semana y 24 horas al día tenemos a gran parte del personal del MCCE participando en esta operación, donde nuestro esfuerzo principal es la defensa de la red sanitaria del Ministerio de Defensa. Protegemos y defendemos continuamente las redes y sistemas del Hospital Central de la Defensa *Gómez Ulla*».

Simultáneamente, el MCCE es el Mando Operativo Ciberespacial de las operaciones permanentes de la Fuerza Conjunta. Asimismo, ejerce la dirección operativa de los Centros de Operaciones de Seguridad del Ministerio de Defensa; y conforma el Centro de Respuesta ante Incidentes de Ciberseguridad del Departamento, con la denominación CERT de Defensa (ESPDEF-CERT). Por ello se está en contacto continuo con los otros dos CERT gubernamentales (INCIBE-CERT y CCN-CERT), contribuyendo al Sistema Nacional de Seguridad en este ámbito. «La coordinación y el trabajo en equipo son las claves para garantizar un ciberespacio seguro y fiable», afirma el jefe del Estado Mayor del MCCE.

Las amenazas en la red tienen una importancia clave en las operaciones militares



El entrenamiento y la dedicación diaria mejoran la preparación de los militares destinados en la unidad para hacer frente a las amenazas en las redes.

Ciberseguridad en la zona gris y las guerras asimétricas

Contralmirante
Javier Roca Rivero
Segundo Comandante
del MCCE

LOS avances tecnológicos y las conquistas sociales de las últimas décadas, sumado a la creciente aversión al conflicto físico, supondrán que el ámbito ciberespacial y el ámbito cognitivo se transformarán en los nuevos y predominantes «campos de batalla» para resolver disputas internacionales que antes se resolvían mediante el intercambio de fuego entre fuerzas convencionales.

En la nueva era digital, se está implantando una nueva forma de confrontación militar. En lugar de centrarse en la destrucción física de las fuerzas enemigas, utilizando el desgaste o la maniobra, se buscan los puntos críticos del adversario para colapsar su funcionamiento y hacerlo incapaz de atacar, protegerse o actuar en defensa de sus intereses nacionales. Idealmente, lo dejará «ciego, sordo y mudo» y sin libertad de acción alguna.

El ciberespacio es ya un dominio real y, sin ningún género de dudas, el entorno operativo más demandante y cambiante en el que operan nuestras Fuerzas Armadas. Es el paradigma de la guerra asimétrica y el entorno ideal para la ejecución de muchas de las actividades asociadas con la llamada «zona gris». El Mando Conjunto del Ciberespacio proporciona unas capacidades diferentes a las fuerzas que operan en los ámbitos físicos, y en las crisis del futuro ofrecerá unas opciones de respuesta militar no solo diferentes, sino que, a veces, serán las únicas posibles.

Como las actividades en la zona gris afectan a todo el Estado, la mejor forma de actuar es trabajar en coordinación y colaboración con todos los actores estatales en el ciberespacio (DSN, CCN, INCIBE, OCC, CNPIC y las FCSE). Mostrar un frente unido (unidad de acción), compartir información, experiencias, alerta temprana coordinada entre todos y reacción rápida y preplaneada son la mejor opción para combatir en el ciberespacio. El MCCE así lo demuestra y practica todos los días. Como decía el maestro Sun Tzu en su obra más famosa: «El supremo arte de la guerra es someter al enemigo sin luchar».

ADIESTRAMIENTO

Los miembros del MCCE se preparan para su labor con entrenamiento y dedicación, y sobre todo con el trabajo diario en el Centro de Operaciones de Ciberseguridad del Ministerio de Defensa, herramienta principal del ESPDEF-CERT. En 2020, el ESPDEF-CERT operado por el Mando Conjunto del Ciberespacio analizó 713 *ciberincidentes* de los miles de recibidos en redes y sistemas del Ministerio, casi dos al día, lo cual es significativo, ya que los motivos para analizarlos fueron la complejidad del incidente o el número de usuarios a los que iban dirigidos.

Siguiendo la máxima de «adiéstrate como combates», el Mando ha incrementado notablemente su Plan de Actividades de la Fuerza, participando en numerosos ejercicios nacionales e internacionales.

«Los ejercicios permiten a nuestros grupos de la Fuerza de Operaciones en el Ciberespacio —señala su comandante, el coronel Francisco Palomo— mejorar sus habilidades en la defensa de las redes y sistemas nacionales e infraestructura crítica contra ataques en tiempo real, así como ejercer la oportuna respuesta». El enfoque se centra en escenarios realistas, tecnologías de vanguardia y en experimentar toda la complejidad de un ciberataque masivo, incluyendo aspectos estratégicos de toma de decisiones, legales y de comunicación. La FOCE es la única unidad de la Fuerza que se encuentra bajo dependencia orgánica del JEMAD y permanentemente integrada en la estructura operativa de las FAS.

En el ámbito nacional, el MCCE participa como Mando Componente Ciberespacial en *Copex 21*, actividad de adiestramiento del Mando de Operaciones junto con sus Mandos Componentes ante una situación de actuación inmediata en un país desolado por una catástrofe natural. Además, es parte importante en el ámbito ciberespacial de los ejercicios *Marsec* de la Armada y *Toro* del Ejército de Tierra; y este año en *Steadfast Leda 21*, durante la evaluación del Cuartel General de Despliegue Rápido de la OTAN en España de Bétera para dirigir operaciones de alta intensidad (*Warfighting Corps*).

En el exterior, el Mando interviene anualmente en *Cyber Coalition*, el mayor ejercicio de ciberdefensa organizado por la OTAN; y en *Locked Shields*, organizado por el Centro Cooperativo de Excelencia de la OTAN en Ciberdefensa, ubicado en Estonia, que ofrece el desafío técnico de ciberdefensa real más complejo del

El MCCE es el resultado de la fusión del anterior Mando Conjunto de Ciberdefensa con la Jefatura CIS

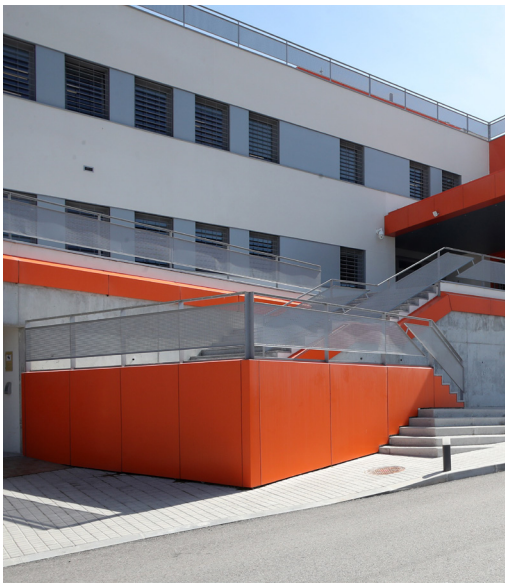
La importancia de la concienciación

La vulnerabilidad informática más importante de casi todas las organizaciones está en el personal que no conoce las medidas de seguridad elementales para no facilitar un ataque de manera inconsciente. Las principales maneras de introducirse en una red (lo que en el MCCE llaman «vectores de ataque») tienen nombres extravagantes como *Phishing, Smishing, Watering-Hole, Man-In-The-Middle o Living off the land*. Es imprescindible que los usuarios sepan cuáles son estas formas de ataque y se puedan prevenir de ellas. Una vez que los intrusos han comprometido la cuenta de un usuario (por poco importante que pueda parecer este), el éxito del ataque se facilita mucho, ya que les permite hacer movimientos laterales dentro de la red y comprometer otras cuentas y otros recursos.

En relación coste-beneficio, la inversión que más favorece la resiliencia y la seguridad de una red es la concienciación de sus usuarios, una tarea para la que se necesita disponer tanto de conocimientos técnicos como habilidades de comunicación, de diseño de imagen y audiovisuales.

Por todo ello, y como prioridad, el MCCE dirige la concienciación de todo el Ministerio de Defensa. Además de elaborar mensajes mediante correo electrónico a todo el personal con consejos generalistas de seguridad en el ciberespacio, se lanzan mensajes más concretos que alertan de ataques en curso. Muy a menudo se trata de los mismos ataques que recibe cualquier gran empresa o el público general en sus correos electrónicos. Adicionalmente, se dan conferencias al personal que ocupa puestos clave, como los que van a participar en alguna misión o los agregados militares que relevan en las Embajadas.

En los últimos meses también se han dado numerosas conferencias al personal sanitario de Defensa para ayudarlos a protegerse de ataques como los que han ocurrido tanto en hospitales civiles españoles como en el extranjero. En la misma línea, se está desarrollando una campaña informativa con el mensaje: «En las redes, prevenir es mejor que curar». Inicialmente, está dirigida a los sanitarios, pero se espera ampliar el foco para alcanzar a más personal.



La unidad participa en la Misión Baluarte contra el coronavirus como Mando Componente Ciberespacial

mundo. Además, recientemente se realizó el primer ejercicio de ciberdefensa de la UE, organizado por la Agencia Europea de Armamento (EDA), que surge de la necesidad de coordinar las actuaciones y el apoyo mutuo entre los CERTs militares de los países que conforman la Unión Europea; el MCCE, como CERT militar de España, quedó el quinto entre los dieciocho participantes.

Cada dos años se organiza el ejercicio nacional *Ciber Bastión*, principal ciberejercicio nacional del Mando Conjunto del Ciberespacio, que se emplea para probar y adiestrar la doctrina nacional en este tipo de operaciones.

En todos estos ejercicios se tiene la sensación real de que los incidentes están ocurriendo y de que existen varios *red teams* enemigos que usan su ingenio y capacidades para derrotar al Mando. La colaboración internacional es algo necesario que incluso se valora en la puntuación final.

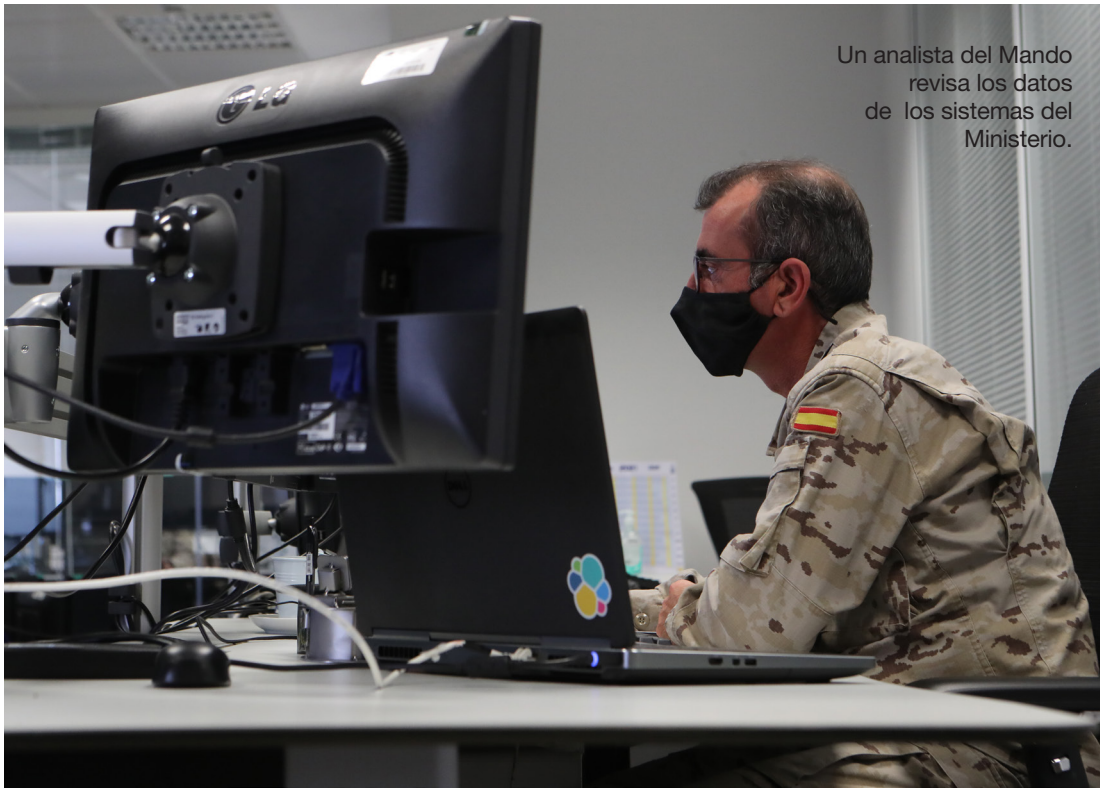
Además, los especialistas del MCCE intervienen en numerosos foros y conferencias, nacionales e internacionales, militares y civiles. «No en vano, somos el representante del Ministerio de Defensa en el Consejo Nacional de Ciberseguridad», concluye el coronel Francisco Palomo.

RETO TECNOLÓGICO

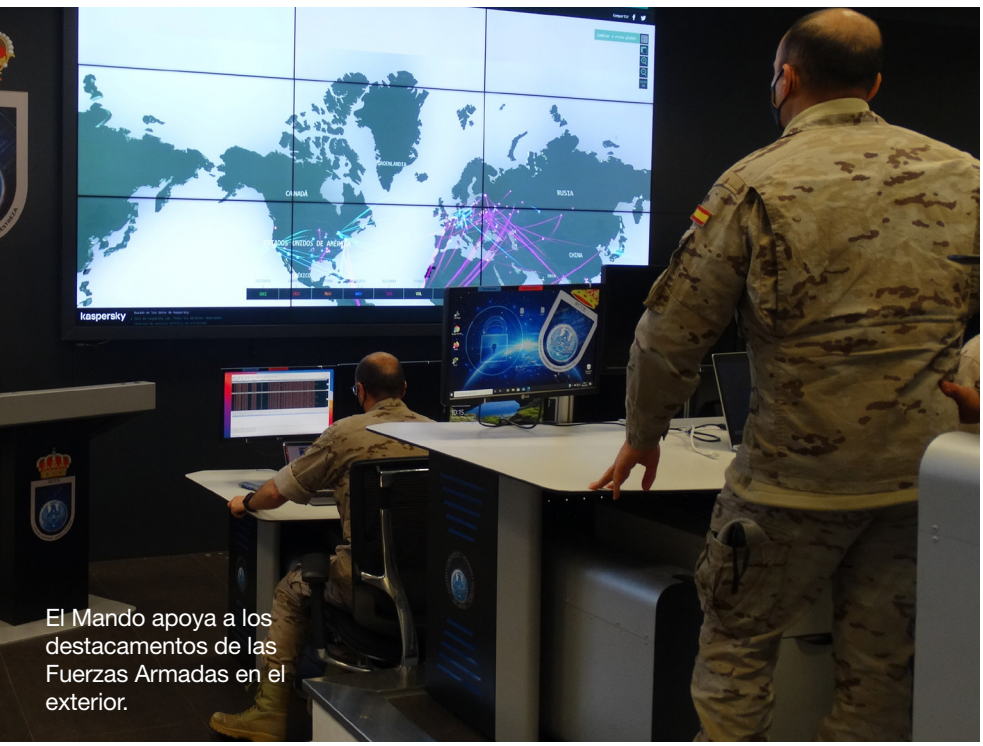
El Mando cuenta con una Jefatura de Sistemas de Ciberseguridad (JSCD), que tiene como una de sus misiones más relevantes la gestión de I+D+i en lo relativo a la ciberdefensa, mediante un proceso que abarca distintas áreas de acción. Una de ellas consiste en definir las líneas de investigación en el ámbito de las capacidades de ciberdefensa. Estas líneas posteriormente se traducen en proyectos de I+D+i, enmarcados en una política común, que se ejecutan con la Dirección General de Armamento y Material (DGAM), y en los que el MCCE ejerce la dirección técnica.

Esta Jefatura actúa también como observatorio tecnológico en ciberdefensa, que aborda tanto la vigilancia como la prospectiva, con dos objetivos principales: estar al tanto de las tecnologías relacionadas con ello, para poder definir las líneas de investigación; y conocer de primera mano todas las familias de productos que pueden ser útiles para el MCCE y las FAS, en

Sede del Mando Conjunto del Ciberespacio, en la base de Retamares.



Un analista del Mando revisa los datos de los sistemas del Ministerio.



El Mando apoya a los destacamentos de las Fuerzas Armadas en el exterior.

MCCE

estrecho contacto con la Jefatura de Sistemas Satelitales y de Ciberdefensa de la DGAM. En esta misma línea se dispone de un área de evaluación de tecnologías, encargada de probar los productos con el fin de comprobar su validez. Para ello, se apoya en el Campo de Maniobras (*Cyber Range*), pudiendo ejecutar todo tipo de ensayos, tanto de funcionalidad e interoperabilidad como de seguridad, en entornos simulados y escenarios que se acerquen lo máximo posible a la realidad de las redes y sistemas del Ministerio.

Gracias a esta experiencia, como señala el coronel José Raúl Gómez Bas, jefe de la JSCD, este órgano «plantea arquitecturas y tecnologías comunes, interoperables, de forma transversal, apoyando además en la definición de requisitos, diseño e implantación cuando sea necesario».

El área de evaluación de tecnologías prueba los productos de I+D+i en ciberdefensa

Además, la Jefatura de Sistemas de Ciberseguridad apoya al resto de jefaturas con asesoramiento técnico especializado en ciberdefensa sobre diversos temas de amplio espectro: desde tecnologías emergentes y disruptivas, como inteligencia artificial, *Blockchain* o 5G, hasta funciones más clásicas de la seguridad, como análisis de riesgos y seguridad de la información en los sistemas. Asimismo, proporciona el apoyo técnico de ingeniería que requieren los grupos de Defensa, Explotación y Respuesta de la Fuerza de Operaciones en el Ciberespacio, lo cual implica tanto el diseño, desarrollo y evolución de productos y sistemas dirigidos a la obtención o mejora de capacidades, como la participación en ciberejercicios para la puesta en práctica de las mismas.

Gema Nieves
Fotos: Pepe Díaz