General de división Rafael García Hernández, comandante del MCCE

«LAS OPERACIONES EN EL CIBERESPACIO PODRÁN PREVENIR GUERRAS»

Destaca que las personas son el elemento más vulnerable a los ataques cibernéticos

DESDE agosto de 2020 está al frente de la unidad más joven de las Fuerzas Armadas, el Mando Conjunto del Ciberespacio (MCCE), responsable de asegurar la libertad de movimientos en este nuevo campo de batalla. Lo que en él ocurre «afecta a todo tipo de operaciones, sean terrestres, aéreas, navales o espaciales», afirma el general de división Rafael García Hernández. «Es un enemigo que ha venido para quedarse», asegura. Prueba de ello son los 700 ciberincidentes analizados, de los miles que se detectaron el año pasado en el ámbito militar, debido a la importancia y complejidad de estos. «La mayoría se deben a simples configuraciones erróneas de equipos; solo un 10 por 100 son ataques de *maleware*, idénticos a los que sufre la sociedad civil y fáciles de parar», tranquiliza el comandante de esta unidad dependiente del JEMAD.

Además de la ciberdefensa, el MCCE tiene atribuciones en materia de guerra electrónica y de mando y control, campo este último al que el general García Hernández ha dedicado gran parte de su trayectoria profesional en el Ejército del Aire. «Es el *background* que me ha traído hasta aquí», señala. «En nuestra época no había cursos de ciberdefensa. Entonces creíamos que el ciberespacio no existía».

—¿Cuál es la misión del MCCE?

—La razón de ser del Mando es garantizar el libre acceso al ciberespacio, asegurar la disponibilidad, la integridad y confidencialidad de la información y de las redes y, en definitiva, asegurar la libertad de acción de las Fuerzas Armadas en este ámbito.

—Antes se llamaba Mando Conjunto de «Ciberdefensa» ¿Por qué se le cambió el nombre?

—El ciberespacio es un concepto más amplio porque, desde el punto de vista de las operaciones, la capacidad de ciberdefensa va unida a las de guerra electrónica y mando y control, que antes eran campos de actuación de la Jefatura CIS de las Fuerzas Armadas y ahora se han incluido en una misma unidad.

«Quien domine el ciberespacio y limite la libertad de acción del oponente, dominará la contienda»

—¿Qué importancia tiene hoy día el dominio de las redes?

—El ciberespacio es una zona de operaciones en permanente actividad, un entorno donde actores con diferentes intereses actúan contra los intereses de los estados. Es un ámbito más de las operaciones militares, transversal al resto de los ámbitos terrestre, aéreo, naval o espacial. En un futuro muy próximo, en el que las operaciones se desarrollarán en un entorno multidominio, donde todo va a estar interrelacionado, el control del ciberespacio será imprescindible para poder operar en esos otros ámbitos físicos o incluso en el cognitivo. Quien domine el ciberespacio y limite la libertad de acción del oponente, dominará la contienda. Las operaciones en el ciberespacio podrán prevenir guerras.

—¿Se previene a los militares sobre el uso de sus redes sociales, sus teléfonos...?

—Desde el primer momento de la creación del MCCD, en 2013, a hoy como MCCE, uno de los cometidos que se le asignaron al Mando fue el de ser responsable de la concienciación en el ámbito ciberespacial. Siempre hemos tenido claro que el elemento más vulnerable del sistema son las personas, por eso se diseñan y difunden campañas de


MCCE
GARCIA HERNANDEZ A.

concienciación para el personal del Ministerio de Defensa que engloban todos los aspectos de la exposición en internet, redes sociales, telefonía móvil, correos electrónicos, así como medidas de seguridad en el uso de la red de propósito general del Ministerio, tanto en territorio nacional como en operaciones internacionales.

Los que se van a misiones en el exterior asignados a puestos clave o, por ejemplo, a una agregaduría de Defensa en el extranjero, reciben charlas y conferencias de concienciación específicas.

—¿Se han incrementado los ciberataques con la pandemia?

—Sí. Se ha visto un repunte en el número de ciberataques y un avance en la complejidad de estos, además con una temática orientada a asuntos COVID.

—¿Hay forma de prevenirlos?

—La colaboración entre todos los actores y los Centros de Operaciones de Ciberseguridad de las diferentes ministerios, la concienciación y alertar a los usuarios sobre las medidas básicas de seguridad, son las medidas más eficaces en cuanto prevención.

—¿Qué habilidades debe dominar el personal de este Mando?

—Por un lado, tenemos perfiles de carácter genérico para aquellas tareas transversales a todas las unidades (personal, logística, Estado Mayor, inteligencia…). Por otro lado, tenemos perfiles específicos del área TIC/Ciber, para atender los asuntos propios del ciberespacio, guerra electrónica, telecomunicaciones, ciberdefensa, satélites y mando y control. En concreto, los del área ciber se forman con cursos básicos, avanzados y de especialización en diferentes áreas.

—¿Participan en actividades en el ámbito de la OTAN?

—Así es. Representamos al Ministerio de Defensa en el Centro Cooperativo y de Excelencia de Ciberdefensa de la OTAN, con sede en Tallín, Estonia. Este centro desarrolla proyectos de investigación sobre aspectos técnicos, operativos, estratégicos y legales en el ámbito ciberespacial, y programan ciberejercicios, como *Locked Shields* y *Crossed Swords*, que permiten el adiestramiento en un entorno muy cercano a la realidad. Participamos en el desarrollo de estos proyectos y ejercicios y también aprovechamos la oportunidad que nos proporcionan de asistir a cursos sobre estas materias.

—¿Existen iniciativas similares en la Unión Europea?

—En la esfera de la UE colaboramos en una serie de proyectos PESCO y participamos en ejercicios que programa y desarrolla la Agencia Europea de Defensa (EDA). Por ejemplo, en febrero hemos participado en el MIC21 (*Military CERT interoperability Conference 21*) donde los CERT Militares de 17 países de la Unión Europea más Suiza competimos en un ejercicio de defensa de redes, y nuestro CERT quedó en quinta posición.

Esto en lo que se refiere a la parte ciber, pero el MCCE también representa al Ministerio de Defensa en la OTAN y UE en otras áreas de trabajo, como las de mando y control, telecomunicaciones y guerra electrónica.

—¿Se contempla también la colaboración con sus equivalentes civiles en situaciones excepcionales?

—Sí. De hecho ya ha habido algunas colaboraciones a petición de otros ministerios, como fue en la Cumbre del Clima COP 25 o durante los diferentes procesos electorales de 2019. En esos casos apoyamos a la Oficina de Coordinación de Ciberseguridad de la Secretaria de Estado de Seguridad en la detección de amenazas que pudieran afectar al buen desarrollo de los mismos.

Aparte, existen planes de colaboración, también a petición de otros ministerios, en la protección de infraestructuras críticas. A esto hay que añadir las relaciones de colaboración que existen entre los diferentes actores estatales con responsabilidad en el ciberespacio. En diciembre del año pasado, el Mando de Operaciones organizó el *I Seminario de Apoyo de las FAS a las Autoridades Civiles en un entorno de Zona Gris*. El MCCE lideró el grupo de trabajo para la colaboración en el ciberespacio, en el que hubo representantes del Departamento de Seguridad Nacional, el Centro Criptológico Nacional, INCIBE, la Oficina de Coordinación de Ciberseguridad, Policía Nacional y Guardia Civil.

El seminario fue valorado muy positivamente por todos los participantes como una oportunidad de mejorar el conocimiento mutuo, que es lo que permite una mejor colaboración. Una de las conclusiones a las que se llegó es que la contribución de las Fuerzas Armadas, en este caso el MCCE, es muy valiosa por las capacidades que puede aportar.

«Con la pandemia se ha visto un repunte en el número de ciberataques y un avance en la complejidad»

José Luis Expósito
Fotos: Pepe Díaz