El JEMAD, acompañado por el director del CESEDEN y el jefe del Mando Conjunto de Ciberdefensa, en la clausura de las jornadas.

Conciencia nacional de CIBERDEFENSA

El Mando Conjunto convoca en el CESEDEN a todos los que trabajan por la seguridad en este ámbito

AHORA se está combatiendo en el ciberespacio; algunos están triunfando y otros están siendo derrotados». Las palabras del jefe de Estado Mayor de la Defensa, Fernando García Sánchez, pronunciadas a principio del mes de abril en el Centro Superior Estudios de la Defensa Nacional (CESEDEN) en el marco de las jornadas *Construyendo la Ciberdefensa en España* hacían referencia a una realidad que todavía algunos no perciben o no le dan la importancia que merece. El JEMAD alertaba de las amenazas que sacuden a diario, muchas veces sin darnos cuenta, ese nuevo campo de batalla constituido por un conjunto de tecnologías, redes, ordenadores e infraestructuras que deben ser protegidas de manera conjunta, es decir, por civiles y militares, si se quiere «garantizar el funcionamiento de los países, el bienestar de los ciudadanos y la Seguridad Nacional», como afirmó el general de brigada Carlos Gómez López de Medina, comandante del Mando Conjunto de Ciberdefensa. Dar respuesta o anticiparse a los ciberataques militares es el cometido principal de este organismo dependiente del JEMAD. Pero no el único. Otro de sus objetivos es promover la conciencia nacional en este ámbito.

Celebrado durante cuatro días, entre el 31 de marzo y el 3 de abril, uno de los aspectos más destacados del encuentro fue la participación del sector industrial, especialmente el privado. Un total de 39 empresas presentaron 44 propuestas de participación. Finalmente fueron elegidas cuatro —Deloitte, Hewlett-Packard, S21 Sec y Dino Sec— para exponer mediante demostraciones prácticas cómo enfrentarse a diferentes amenazas en escenarios muy diversos.

El sector académico estuvo representado en las jornadas por las Universidades Politécnica, Complutense y Rey Juan Carlos de Madrid y la de Alcalá de Henares. Por parte de la administración, acudieron al CESEDEN representantes de los ministerios de la Presidencia, Defensa, Industria e Interior y de la Fiscalía General del Estado dedicados a la ciberseguridad.

CONFLICTO PERMANENTE

«Ante un gran ataque en el ciberespacio, no volveríamos a los 80, sino a principios del siglo pasado», aseguró el ministro de Defensa, Pedro Morenés, en el acto de inauguración de las jornadas. «El ciberespacio —añadió— es el elemento básico de comunicación y de gestión de las sociedades humanas. Estamos descubriendo un ámbito que era desconocido no más allá de 25 años y que hoy puede ser motivo de las agresiones más brutales que puede recibir una sociedad».

La reciente creación del Mando Conjunto de Ciberdefensa responde a esa realidad. Está enfocado, apuntó Pedro Morenés a «la necesidad de dotar a la Defensa Nacional, especialmente a las Fuerzas Armadas, de las capacidades necesarias para defender a nuestra organización de cualquier ataque que pudiera debilitarla», así como dotarla de las herramientas que permitan anticiparse a esos ciberataques. Para alcanzar este objetivo «es imprescindible contar con el sector industrial e intelectual del país». Es la propuesta que hizo el ministro de Defensa a los asistentes a estas jornadas.

En opinión del capitán de navío Enrique Cubeiro, jefe de Operaciones del Mando Conjunto de Ciberdefensa, existen actores en el ciberespacio que poseen capacidad técnica para provocar muchos estragos en un amplio espectro. «Muy pocos pueden hacer mucho daño y, por tanto, la ciberguerra es el paradigma de la guerra asimétrica». Cubeiro considera también que, en este ámbito, el esfuerzo del defensor es mayor que el que pueda realizar el agresor: «la ciberdefensa es mucho más cara y compleja que el ciberataque. Además, cuanto más tecnicodependiente es una nación, una organización o un ejército, más vulnerables serán a este tipo de agresiones».

Más adelante, aseguró que existe un considerable vacío legal en el ciberespacio. «Esta ausencia de autoridad favorece al agresor y hace que la trazabilidad del ataque y su origen sean muy difíciles de controlar». Por su parte, los docentes universitarios también se

«En la defensa del ciberespacio es necesario contar con el sector industrial e intelectual del país», señaló Morenés

mostraron unánimes al asegurar que el tratamiento específico de esta cuestión debe abordarse en profundidad en los estudios de postgrado o, como ocurre en la actualidad, en los 17 máster dedicados a esta especialidad.

Hasta no hace mucho tiempo, los contenidos universitarios sobre seguridad de la información estaban centrados en la criptografía. Ahora se enseñan otras asignaturas como auditoría, seguridad en redes o análisis de riesgos. El abanico es cada vez más amplio, pero siguen sin estudiarse en las áreas de la informática y las telecomunicaciones cuestiones como el análisis forense y el desarrollo seguro de la información. Según los especialistas, en los 93 estudios de grado dedicados a esta materia solo se aborda el aspecto técnico de la seguridad de la información, mientras que la ciberdefensa se estudia en profundidad en el postgrado o en los 17 máster de esta especialidad que se ofertan actualmente.

A las jornadas asistieron especialistas militares, de los ámbitos universitario y empresarial y de la Administración del Estado.

COCIENCIACIÓN

El acercamiento de todos los colectivos implicados fue uno de los aspectos debatidos en la mesa redonda dedicada a *La concienciación en ciberseguridad. Modelos efectivos*, cuyo objetivo fue «agitar conciencias para ver cómo se puede resolver esta cuestión», apuntó su moderador el comandante Luis Herrero, jefe de la sección de Formación del Mando Conjunto. En este encuentro participaron representantes del Instituto Nacional de Tecnologías de la Comunicación (INTECO) y del Centro Criptológico Nacional del Centro Nacional de Inteligencia. La mesa redonda también contó con la presencia del sector docente. Desde la Universidad Complutense, Eduardo Huedo, profesor de Seguridad de Redes de la Facultad de Informática, se quejó de que no existe una estrategia en Educación, es decir, un modelo de actuación «para concienciar a los alumnos en materia de ciberseguridad ya que en Primaria y Secundaria no hay ingenieros informáticos o de telecomunicaciones que les formen». A su juicio, «la cuestión de la seguridad en este ámbito no está bien planteada», como sí lo está en las Fuerzas Armadas a través del Mando Conjunto de Ciberdefensa; en las Fuerzas y Cuerpos de Seguridad del Estado que disponen, entre otras, de unidades de delitos telemáticos; en la Administración donde destaca la labor que en este ámbito realiza el Centro Criptológico Nacional; y, de manera más reciente, «en las empresas más tecnológicas, conscientes de los riesgos de seguridad», afirmó el profesor Huedo. Precisamente el jefe de Estado Mayor de la Defensa abogó durante la clausura de estas jornadas por impulsar la difusión de los temas relacionados con la ciberseguridad y la ciberdefensa en los sectores educativos y en otros donde aún no se aprecia la importancia de esta cuestión.

Para el almirante general Fernando García Sánchez, el encuentro del CESEDEN sirvió para implicar a los sectores público y privado, empresarial, de la enseñanza universitaria y de la Administración. «Esta coordinación y colaboración es fundamental para avanzar en este ámbito», destacó el JEMAD tras señalar que se trata de un objetivo contemplado en la Estrategia de Ciberseguridad Nacional.

En opinión del JEMAD otro de los aspectos que hay que impulsar a través de encuentros como éste es el de «mostrar y demostrar que existen capacidades tecnológicas industriales en el ámbito de la ciberdefensa y que se pueden utilizar medios que se desarrollen con carácter nacional para resolver problemas de ciberseguridad, que muchas veces son de carácter global o general».

El almirante general García Sánchez también valoró muy positivamente el trabajo conjunto que se está realizando en el marco de la Administración. «El Centro Criptológico Nacional, el INTECO, el Consejo Nacional de Infraestructuras Críticas, las Fuerzas y Cuerpos de Seguridad del Estado y el Mando Conjunto de Ciberdefensa pueden y están trabajando juntos para que la estrategia de ciberseguridad de resultados positivos a corto, medio y largo plazo», afirmó. El JEMAD señaló la necesidad de impulsar el plan de acción del Mando Conjunto de Ciberdefensa.

«Es un elemento clave desde el punto de vista militar y de la ejecución de las operaciones», y fundamental para que «ese trabajo de siete días, 24 horas, permita controlar esas cuestiones pequeñas que ocurren a diario en este nuevo campo de batalla que es el ciberespacio y, en el caso de que tengamos alguna situación más grave, podamos colaborar todos de la manera pertinente en su resolución».

J.L. Expósito
Fotos: Hélène Gicquel