General de brigada Carlos Gómez López de Medina
Comandante del Mando Conjunto de Ciberdefensa

«El control del ciberespacio es un objetivo muy ambicioso»

El mando, bajo dependencia directa del JEMAD, ha nacido para proteger los sistemas conjuntos de información y de telecomunicaciones de las Fuerzas Armadas

DESDE hace apenas tres meses el general de brigada Carlos Gómez López de Medina opera en un escenario que podría calificarse, cuando menos, de ambiguo, porque es muy difícil de acotar, ya que carece de fronteras físicas, y en el que resulta muy complicado ubicar y poner cara al enemigo. El pasado 3 de julio fue designado comandante jefe del Mando Conjunto de Ciberdefensa de las Fuerzas Armadas. La unidad, que alcanzó la capacidad operativa inicial el pasado 27 de septiembre con 25 militares y 10 civiles —los primeros de una plantilla de 70— ha sido creada para la defensa de las redes y los sistemas conjuntos de información y de telecomunicaciones militares en el ciberespacio. Se trata de un nuevo escenario de confrontación, «tanto —dice el general Medina—, que carece todavía de reglas de enfrentamiento», no existe doctrina sobre el mismo y jurídicamente está muy poco definido. Su campo de batalla también es distinto a los cuatro tradicionales de la guerra convencional: terrestre, marítimo, aéreo y espacial.

El general Medina, granadino de 55 años, fue ayudante de campo de S. M. el Rey siendo teniente coronel, pero el hilo conductor de su trayectoria profesional ha sido el Mando y Control Aéreo con 21 años de servicio dedicados a este ámbito en España y en la sede de la Alianza Atlántica en Bruselas.

—General, ¿Cómo definiría usted el ciberespacio militar?

—El conjunto de Sistemas de Información y de Telecomunicaciones que son de interés para las Fuerzas Armadas, desde, por ejemplo, el de mensajería oficial y gestión documental del Ministerio de Defensa (SIMENDEF) hasta el de información del jefe de Estado Mayor de la Defensa (SIJE). No se trata tanto de que el ciberespacio sea de interés militar, sino de tener libre acceso al mismo para procurar un bien nacional utilizando un instrumento como las Fuerzas Armadas al servicio del Estado.

«Además de los sistemas propios, también nos interesan los del adversario»

Es un objetivo ambicioso. Además de los sistemas propios también nos interesan los del adversario, su SIMENDEF y, sobre todo, su SIJE.

—¿Estamos quizás ante un nuevo campo de batalla?

—Tan nuevo que no existen todavía reglas de enfrentamiento. El conocimiento se obtiene experimentando. Desde el ciberespacio es posible inutilizar el funcionamiento de una central eléctrica o alterar el estado de la opinión pública mediante una acción de propaganda a través de la generación de una información falsa en las redes sociales como, por ejemplo, en *Twiter* o *Facebook*.

También es posible actuar en combinación con los escenarios de la guerra convencional, generalmente llevando a cabo acciones de inteligencia.

Es difícil, pero no imposible, acceder al sistema de mando y control del adversario y extraer información o alterarla con el objetivo de disminuir su eficacia para favorecer la penetración de nuestras fuerzas convencionales.

El general Medina trabaja ya con 24 militares y 10 civiles en el Cuartel General de Retamares, ubicado en la localidad madrileña de Pozuelo de Alarcón.

—¿Podría decirse que con este mando ha nacido un nuevo Ejército?

—Hoy por hoy no es así, y tampoco me parece necesario que haya que crearlo. El mando se nutre, como cualquier otra unidad de la Fuerza Conjunta, de personal de los tres Ejércitos.

—¿Cuáles son los principales cometidos del nuevo mando conjunto?

—En la Orden Ministerial (10/2013) de creación del Mando figuran nueve. Los principales son, como ya he dicho, garantizar el libre acceso al ciberespacio y la defensa de los sistemas conjuntos de información y de telecomunicaciones militares. Nuestra prioridad son aquellos desplegados en zona de operaciones por ser los más expuestos y encontrarse allí donde tenemos gente asumiendo un mayor nivel de riesgo. Además, la unidad representa al Ministerio de Defensa en los asuntos relacionados con la ciberdefensa, tanto a nivel nacional como internacional.

—¿Cree que se necesita una mayor concienciación y formación en esta materia en las Fuerzas Armadas?

—Sí, es otra de las responsabilidades de este mando. Debemos conseguir que toda persona, con y sin uniforme, que trabaje en el Ministerio de Defensa sea sensible a las amenazas cibernéticas. Realizaremos campañas, intervendremos en cursos y utilizaremos todos los medios necesarios para lograrlo. También es imprescindible que exista formación en ciberdefensa en las academias militares y escuelas especializadas de los Ejércitos y la Armada. Posteriormente, aquellos que sean destinados a este mando se encontrarán con una unidad de transformación que les pondrá en condiciones de cumplir con su misión. Pero antes debemos llegar a una definición adecuada de *Combat Ready*, el perfil del combatiente en cada un de los puestos de trabajo del nuevo mando. Esto es lo que va a condicionar qué tipo de formación va a recibir la persona que ocupe ese puesto de trabajo.

—¿Cuáles serán las áreas básicas de actuación del mando?

—Disponemos de tres capacidades: defensa, explotación de información y respuesta. En primer lugar, cualquier usuario necesita que su sistema informático sea seguro. En nuestro caso debemos estar preparados para la protección de los sistemas de información y comunicacio-

nes frente a los ciberataques y para su recuperación en caso de fallo o inutilización parcial o total. La capacidad de explotación está relacionada con la inteligencia, se trata de penetrar en los sistemas adversarios e investigar qué es lo que hay en ellos. Por último, la capacidad de respuesta es la realización de ciberataques.

La actividad defensiva es común a muchos usuarios por lo que existen soluciones de doble uso que nos sirven a civiles y militares. Sin embargo, cuando hablamos de inteligencia o respuesta no tenemos compañeros de viaje, especialmente en la última porque se trata de una operación típica de las Fuerzas Armadas.

—¿Cómo se acometerá la puesta en marcha de estas capacidades?

—Pretendemos trabajar en paralelo en las tres áreas aunque inicialmente lo haremos con mayor intensidad en defensa, luego en explotación de información y, finalmente, en ataque. Lo más urgente

«La futura estrategia de ciberdefensa requiere una autoridad nacional definida»

para cualquier usuario de sistemas de información es protegerse. Un pequeño grupo bien organizado y con pocos recursos puede enfrentarse a toda una nación y ocupar portadas en los periódicos.

—¿Cuál es *la fuerza de combate* del nuevo mando conjunto?

—La Jefatura de Operaciones es la parte del mando donde se concentran los recursos para desarrollar sus capacidades. Cuenta con tres elementos. Uno es puramente defensivo, otro combina explotación de información y respuesta y el tercero constituye lo que denominamos el grupo técnico. Este tercer elemento es nuestra fábrica de *software*, donde se crean los recursos para proteger, hacer inteligencia o atacar, bien con medios propios o apoyándonos en las empresas del sector.

—La estructura del Mando Conjunto de Ciberdefensa se completa con una asesoría jurídica, ¿por qué razón?

—El jurídico es un tema tremendamente complejo en el ámbito del ciberespacio. Es un escenario muy difícil de acotar, no tiene fronteras. Es muy complicado atribuir responsabilidades o proceder legalmente contra alguien. La gente que se dedica a hacer barrabasadas en este ámbito genera la acción en un determinado punto y, utilizando varios relés, va de servidor en servidor. Es muy importante

poder determinar dónde está el origen del ataque. Se está tratando de encontrar modelos jurídicos en la guerra convencional para trasladarlos a este ámbito, pero hay muchas dificultades. En este punto se hace necesario alcanzar acuerdos a nivel mundial que, sin embargo, todavía no está muy claro que los países quieran adoptar. Parece que nos quedan todavía años de anarquía en este asunto, pero no podemos dejar de trabajar en esta área. Somos una nación de Europa occidental y, en consecuencia, debemos «responder a una agresión en el ciberespacio de manera legítima y proporcionada», como indica la orden ministerial de creación del Mando Conjunto de Ciberdefensa.

—¿Qué supone haber alcanzado la Capacidad Operativa Inicial?

—Que disponemos de ubicación, personal y recursos. Es decir, que ya podemos trabajar con una cierta intensidad. Hemos comenzado con 35 personas de una plantilla total que estará constituida por 70, 49 serán militares y 21 civiles. Para iniciar nuestra andadura hemos asumido las funciones de la Sección de Seguridad de la Información —la célula SIC— del Estado Mayor Conjunto, que ha sido el núcleo de constitución del mando.

—¿Cuántos civiles trabajan en la unidad y qué se espera de su aportación?

—Ahora mismo son diez. Que subamos a 21 es una cuestión presupuestaria, por lo que se incorporarán a la unidad de manera progresiva. Los civiles aportan una capacidad tecnológica muy importante al mando conjunto.

Participan en impartir formación, en acciones de defensa y en la creación de recursos *software*. Lo que no harán nunca es ejecutar una acción ofensiva. En el mando los civiles podrían fabricar ciberarmas, pero no utilizarlas.

Una fórmula que impulsaré todo lo que pueda y en la que tengo muchas esperanzas es la del Reservista Voluntario.

«Debemos responder a una agresión en el ciberespacio de manera legítima y proporcionada.»

Es una opción extraordinaria porque hablamos de especialistas en ciberseguridad que pueden aportarnos mucho.

—¿Necesitará *hackers*?, de los buenos, se entiende.

—Sí, tenemos *hackers* civiles y militares, personas con los conocimientos técnicos necesarios para hacer las tareas que desarrollan estos piratas informáticos, pero que, evidentemente, no lo son.

—¿Cómo debe integrarse el mando en los esquemas de defensa colectiva de la OTAN y de la Unión Europea?

—Participamos activamente como socios, y no todos los miembros de la Alianza Atlántica lo son, en el Centro de Excelencia en Ciberdefensa en Tallín (Estonia). Formamos parte de su escuela y de su foro de investigación. La Unión Europea también es sensible a la ciberdefensa, pero avanza más despacio.

—¿Cuáles deben ser las claves de la futura Estrategia Nacional de Ciberseguridad?

—El concepto de estrategia nacional de ciberseguridad nos sobrepasa. En este ámbito convergen numerosos organismos. Hablamos de seguridad nacional. En mi opinión, lo más crítico es la organización de ese dispositivo. Debemos construir una estructura eficaz y eficiente que consiga sus propósitos con el menor coste posible. Es decir, que no estemos haciendo varios lo mismo mientras que hay otras áreas de las que no se ocupa nadie. Esto implica la existencia de una autoridad definida a nivel nacional.

—¿Qué relación tendrá el mando con los centros de respuesta a incidentes de seguridad de la información de los Ejércitos, la Armada y del Órgano Central?

—Coordinar y dirigir la actividad de estos centros será otro de los cometidos de la unidad. El Ejército de Tierra, la Armada y el Ejército del Aire se ocupan de sus redes y sistemas de información y telecomunicaciones específicos. Otra cosa es que nos pidan apoyo para atender alguna necesidad puntual. Las acciones de explotación y respuesta son responsabilidad del mando.

—¿En qué tipo de situaciones apoyará este mando a sus equivalentes civiles?

—Tendremos unos protocolos de colaboración para el caso de que necesiten refuerzos. En alguna ocasión podríamos actuar como una Unidad Militar de Emergencias en este ámbito. El cibercrimen, por ejemplo, es competencia del Ministerio del Interior, es decir, de los Cuerpos y Fuerzas de Seguridad del Estado. Pero sí es cierto que a través de labores de inteligencia con fines estrictamente militares o de seguridad nacional podríamos descubrir algún tipo de delito, pero sin buscarlo expresamente. Esa no es nuestra competencia.

J.L. Expósito
Fotos: Pepe Díaz

«Tendremos unos protocolos de colaboración con los organismos civiles para el caso de que necesiten refuerzos»