Carlos Gómez López de Medina

Comandante Jefe del Mando Conjunto de Ciberdefensa

Con una dilatada trayectoria en el Ejército del Aire, el general de brigada Carlos Gómez López de Medina es el primer responsable del Mando Conjunto de Ciberdefensa. Durante su encuentro con *Red Seguridad*, el militar granadino abordó diversas cuestiones, desde la puesta en marcha de la unidad que dirige hasta las ciberamenazas actuales; para combatir a estas últimas, considera vital la concienciación y la formación.

"El Mando Conjunto tiene como fin lograr los propósitos de la Estrategia de Ciberseguridad Nacional"

Tx: E. González y B. Valadés
Ft: E.G.H.

- ¿Cómo se estructuraba la ciberdefensa en España antes de la creación del Mando Conjunto? ¿Qué motivos propiciaron su puesta en marcha?

Las competencias relativas a la ciberdefensa están distribuidas entre el Centro Criptológico Nacional (CCN) y los ministerios de Industria –a través del Instituto Nacional de Tecnologías de la Comunicación (Inteco)–, del Interior y de Defensa.

En el caso de este último, el Mando Conjunto de Ciberdefensa se creó en febrero del año pasado. Pero, con anterioridad, tanto los tres ejércitos como el Estado Mayor de la Defensa (EMAD) y el Órgano Central del ministerio trabajan en dicha materia. Algo lógico si se tiene en cuenta que en las Fuerzas Armadas se vienen utilizando sistemas de información y telecomunicaciones desde hace muchos años; por lo tanto, ya había una preocupación por la fragilidad de los mismos ante las nuevas amenazas.

Todas las partes implicadas destinaron recursos económicos y humanos para tal fin, pero se echaba en falta un uso más eficiente de los medios disponibles y, sobre todo, una mayor coordinación. Esos fueron los motivos que propiciaron la puesta en marcha del Mando Conjunto de Ciberdefensa.

- Actualmente, ¿cuántas personas operan en la unidad? ¿Contemplan ampliar la plantilla a corto plazo?

El objetivo es finalizar el año con un equipo integrado por 70 personas entre militares y civiles. A partir de ahí, nos gustaría seguir contando con más profesionales, claro; pero, de momento, la ampliación de la plantilla la estamos realizando desde una perspectiva progresiva, razonable y realista. Hasta que se produz-

"En la Administración Pública existe numerosa información 'apetecible' para los ciberdelincuentes"

can más incorporaciones, estoy muy satisfecho con quienes trabajan en el Mando Conjunto de Ciberdefensa, ya que poseen un elevado grado de formación.

- ¿Qué objetivos han logrado desde que está operativo el Mando Conjunto de Ciberdefensa?

Sobre todo, una mejor gestión de los recursos, ya que antes existían numerosas duplicidades. También destacaría que se ha alcanzado la capacidad operativa inicial, lo cual significa que desde el principio teníamos medios, personal, instalaciones, etc. Y por lo que respecta a nuestra actividad, entre las tareas más relevantes que llevamos a cabo se encuentran la evaluación y acreditación de sistemas de información, los análisis forenses y los ciberejercicios, muy importantes para hacer frente a posibles ciberataques. En este apartado, hemos progresado mucho en los últimos meses.

- Una vez alcanzada la capacidad operativa inicial, ¿existe una hoja de ruta definida?

Lógicamente, deseamos llegar a lo que denominamos *full operational capability*: capacidad operativa completa. Y para lograrlo, nos centramos en tres líneas o capacidades: la defensa, lo que se conoce como ciberseguridad; la explotación, más relacionada con la inteligencia, saber qué hace el adversario; y la respuesta, basada en el ataque al enemigo mediante distintos enfoques. En cuanto a los plazos para alcanzar esa capacidad operativa completa, tenemos definidos los niveles y las fechas para cumplir nuestros objetivos, pero, lógicamente, no pueden ser de dominio público.

- ¿Cuáles son las principales líneas estratégicas que se han marcado para lograr sus objetivos?

Al hilo de la respuesta anterior, hemos fraccionado nuestros objetivos a corto, medio y largo plazo. De manera inmediata, consideramos muy importante colaborar con el Mando de Operaciones del EMAD y el Centro de Inteligencia de las Fuerzas Armadas (CIFAS). Y también mejorar el concepto de ciberseguridad entre los miembros del Ministerio de Defensa; para ello, es necesario concienciar, formar y adiestrar al personal, algo que estamos realizando en los tres ejércitos junto al Órgano Central del ministerio.

Respecto a esto último, consideramos que la colaboración es vital. Así, más allá del ámbito militar, trabajamos con los ministerios del Interior y de Industria, así como con el Centro Nacional de Inteligencia (CNI). Podría decirse que son nuestros *partners* más cercanos y, de hecho, participamos conjuntamente en jornadas específicas, mesas redondas, etc.

- Ya que se refiere a la colaboración, ¿la unidad coopera con otros países u organizaciones internacionales en materia de ciberdefensa?

Sí. Esta es una actividad que, a su vez, se divide en dos: por un lado, las relaciones bilaterales, que son muchas y estrechas, con las fuerzas armadas de naciones aliadas y, por otro, las que mantenemos con la OTAN y la Unión Europea (UE). Por ejemplo, el Mando Conjunto es socio fundador del Centro de Excelencia de Ciberdefensa de la OTAN, ubicado en Tallin (Estonia) y del que obtenemos muchos beneficios gracias a los ciberejercicios, cursos de formación, trabajos de investigación, etc. Y en el caso de la UE, si bien no se destinan muchos recursos económicos a la materia que nos ocupa, estamos involucrados en algunas iniciativas y proyectos.

- ¿También prestan atención a la colaboración público-privada?

Por supuesto. Colaboramos con la industria nacional solicitando soluciones que satisfagan nuestras necesidades. Valoro mucho a las empresas españolas que se dedican a la ciberseguridad, creo que desarrollan productos propios de una gran calidad y hacemos todo lo posible para potenciar su capacidad porque, lógicamente, nos interesa a ambas partes. Y también me merecen mucho respeto las universidades por su labor de I+D.

El general de brigada Carlos Gómez, dirige el Mando Conjunto de Ciberdefensa desde enero del año pasado. Este órgano ha alcanzado ya la capacidad operativa inicial.

- En nuestro país, ¿cuáles son las principales ciberamenazas actuales a tener en cuenta?

En la Administración Pública existe numerosa información apetecible para ciberdelincuentes que pueden ser contratados por terceros, algo, por otra parte, bastante habitual. Debemos hacer frente a ese peligro e incrementar el tipo de respuesta si los ataques provienen de grupos organizados de ciberterroristas e incluso de un estado.

En el ámbito corporativo, la principal preocupación es, sin duda, el robo de propiedad intelectual. Y si nos referimos a la sociedad en general, el ciberdelito, qué duda cabe, está cada vez más extendido. En este sentido, creo que se debe fomentar la cultura de la ciberseguridad entre los ciudadanos y concienciarlos de los riesgos que conlleva el uso de un ordenador o dispositivo móvil.

- ¿Qué opinión le merece la Estrategia de Ciberseguridad Nacional?

Creo que es un documento tan relevante como la Constitución española. Marca una serie de líneas muy importantes y refleja un principio fundamental: mejorar la ciberseguridad en nuestro país. Todos los objetivos del Mando Conjunto, a los que he hecho referencia anteriormente, persiguen alcanzar los propósitos de la Estrategia y responden a algunas de las ocho líneas de acción contempladas en el documento. Una de ellas, como ha quedado expuesto, es la relativa a la cooperación internacional: colaboración con la OTAN, fortalecer las relaciones con naciones aliadas, etc.

- Hay quienes manifiestan que la III Guerra Mundial se está librando ya y que la misma es de carácter cibernético. ¿Está de acuerdo?

Me cuesta pensar en guerras exclusivamente cibernéticas. Otra cosa es que haya conflictos en los que exista dicho componente. Les expongo un ejemplo muy gráfico y clarificador: cuando en el siglo pasado entró en combate la aviación, ¿significaba que, a partir de entonces, las tropas terrestres carecerían de utilidad? Obviamente, no. El tiempo demostró que las dos divisiones tienen misiones distintas pero complementarias. Ahora sucede lo mismo. Ninguna fuerza es imprescindible y se actúa conjuntamente, pero hay un invitado más: la ciberdefensa. Y esta última se debe tener muy en cuenta para no ser débil y vulnerable en dicho ámbito. ■

El jefe del Mando Conjunto de Ciberdefensa dialoga con Ana Borredá, directora de Red Seguridad, en uno de los momentos de la entrevista.