“Es imposible que un ataque cibernético bloquee totalmente las capacidades de nuestras Fuerzas Armadas”

5-8-2013 Verónica Sánchez Moreno CISDE OBSERVATORIO DE INTELIGENCIA, SEGURIDAD Y DEFENSA.

A mediados de este mes de julio, el general de Brigada Carlos Gómez López de Medina era nombrado comandante jefe del nuevo Mando Conjunto de Ciberdefensa (MCCD); el cuarto pilar, junto con los mandos de Vigilancia Marítima, Defensa Aérea y Operaciones Especiales, de la “fuerza conjunta” de las Fuerzas Armadas españolas.

Este granadino de 55 años, número 1 de su promoción de la Academia General del Aire, es el encargado de dirigir la defensa de las redes y sistemas de información y telecomunicaciones militares ante amenazas o agresiones que afecten a la Defensa Nacional. Y todo ello a coste 0, ya que, como se señala en la orden ministerial de creación del MCCD, ésta no supone “incremento del gasto público”.

Señala el general Gómez que la situación de España respecto a la defensa cibernética “es similar a las naciones de nuestro entorno” y nos agradece la oportunidad “para difundir el conocimiento sobre el MCCD y que los españoles puedan saber que sus Fuerzas Armadas también se ocupan del ciberespacio, colaborando con otros organismos de la Administración, para que la seguridad y libertad de nuestra sociedad no se vean afectadas”.

¿Por qué la necesidad de crear un Mando Conjunto de Ciberdefensa (MCCD) de las Fuerzas Armadas españolas?

La ciberdefensa es más eficaz y más eficiente cuando se plantea de una manera global. Un Mando Conjunto permite planear y dirigir de forma centralizada y obtener mejores resultados con menos recursos.

Comentaba hace pocos días, en un curso de ciberseguridad de la Universidad Complutense de Madrid, que ahora mismo el Mando Conjunto de Ciberdefensa ya tiene “capacidad de defensa, explotación y respuesta, pero hace falta trabajar mucho en las tres”, ¿está ya este Mando completamente operativo o le hace falta un poco de “rodaje” para alcanzar la plena operatividad?

El Mando necesita recorrer un proceso de mejora de capacidades operativas. Está previsto alcanzar la “Initial Operational Capability” (IOC) a finales del próximo mes de septiembre. Después de la IOC, el Mando seguirá trabajando para alcanzar la “Final Operational Capability” (FOC) en Defensa, Explotación y Respuesta lo antes posible.

¿Qué tipo y cuántos profesionales componen este Mando?

Está previsto que el Mando disponga de 70 personas (49 militares y 21 civiles). Los componentes del MCCD realizarán una amplia variedad de cometidos, destacando entre ellos la evaluación permanente de nuestros sistemas para adecuar su defensa a las amenazas existentes. Las características comunes en el personal perteneciente al MCCD serán los conocimientos y la experiencia operativa y técnica en sistemas de información y telecomunicaciones.

Siguiendo con la pregunta anterior, ¿qué adiestramiento debe recibir un soldado para convertirse en "cibersoldado"?

El necesario y suficiente para que pueda realizar su misión. Si nos quedamos cortos no podrá realizarla y si nos pasamos, estaremos malgastando recursos económicos y tiempo. Es muy importante definir el perfil de conocimientos que debe tener nuestro cibersoldado según el puesto de trabajo que va a desempeñar. Ese perfil nos va a permitir definir el proceso de formación para ocuparlo y el adiestramiento posterior para mantener las condiciones operativas necesarias.

El Mando Conjunto de Ciberdefensa depende directamente del Estado Mayor de la Defensa, para su funcionamiento ¿es importante que haya una buena coordinación entre ustedes, los ejércitos y la Unidad Militar de Emergencias?

El MCCD depende directamente del Jefe de Estado Mayor de la Defensa (JEMAD). Esa coordinación es fundamental para utilizar los recursos existentes de la manera más eficaz y eficiente posible. La coordinación entre todos los organismos del Ministerio de Defensa es imprescindible para que todas las necesidades queden cubiertas y no haya duplicidades.

¿Cuáles son las prioridades del MCCD y los primeros objetivos que se han planteado alcanzar?

Las prioridades fundamentales son alcanzar las IOC y FOC. Los objetivos para 2013 son: alcanzar la IOC, operar con el Mando de Operaciones (MOPS) y el Centro de Inteligencia de las Fuerzas Armadas (CIFAS), obtener la aprobación del presupuesto económico para 2014, iniciar y/o mejorar la coordinación con los organismos con los que el MCCD debe tener relación y dar a conocer el MCCD dentro y fuera del Ministerio de Defensa.

Hoy en día, todas las acciones de guerra convencional se acompañan de ciberataques, ¿cómo ha sido el incremento de este tipo de agresiones y en qué ha influido a las naciones a la hora de realizar estrategias de defensa?

En general, los sistemas de información militares están mejor protegidos que los civiles porque en su diseño y operación se tienen muy presentes la seguridad del propio sistema y de la información que contiene y maneja. La amenaza aumenta porque lo hace el número de posibles agresores que, a su vez, disponen de mayores capacidades tecnológicas para hacerlo. Las acciones ofensivas o de inteligencia en el ciberespacio son muy rentables para el agresor, que "tiene mucho que ganar y muy poco que perder". No

protegerse ante esta amenaza, cada vez más probable, sería una peligrosa falta de responsabilidad que podría tener importantes consecuencias negativas.

¿Cuánto daño pueden hacernos "los malos" en una guerra virtual?

Depende de la capacidad de los "malos", del nivel de protección de nuestros sistemas y de nuestro grado de preparación para hacer frente a los ciberataques y recuperarnos rápidamente. Mucho daño si todo esto está en contra y poco si está a favor.

¿Hasta qué punto puede un ataque cibernético bien diseñado y orquestado bloquear las capacidades de nuestras Fuerzas Armadas?

Actualmente ese bloqueo total es imposible. Los sistemas que utilizamos para planear, dirigir y ejecutar las operaciones militares están diseñados y operados con unos requisitos de seguridad muy exigentes. No obstante, tenemos que seguir trabajando para que este grado de seguridad se mantenga y supere al nivel de evolución de la amenaza.

¿Cree que la creación del Mando Conjunto de Ciberdefensa es la entrada de España en la "guerra moderna" y las nuevas necesidades de seguridad, siguiendo la estela del reciente Centro Europeo de Ciberdelincuencia o de Estados Unidos, que en 2009 creó el U.S. Cyber Command?

Las Fuerzas Armadas Españolas llevan unos años trabajando en ciberdefensa. La creación del MCCD debe aportar una canalización de esos esfuerzos y, en definitiva, un aumento de eficacia y eficiencia. Supongo que ese fue también el motivo que llevó a los EE.UU. a crear su "Cyber Command".

Asimismo, para que el MCCD pueda llevara a cabo sus funciones, ¿se precisa colaboración con otros países?

La coordinación entre aliados es necesaria y muy beneficiosa para todos. Lograrla es uno de nuestros objetivos.

¿Existe conciencia de seguridad cibernética en nuestra sociedad? ¿Se plantean fomentarla de alguna manera?

Hay menos de la que debiera. Según la Orden Ministerial 10/2013, por la que se crea el MCCD, fomentar esa concienciación en el Ministerio de Defensa es uno de nuestros cometidos

General, lleva tres meses trabajando en el Estado Mayor de la Defensa para poner en marcha el Mando Conjunto de Ciberdefensa, ¿qué supone para usted estar al frente de este nuevo reto de las Fuerzas Armadas españolas?

Poner en marcha el MCCD supone para mí una gran responsabilidad y un reto profesional apasionante.