DOSSIER

La Ciberdefensa: un nuevo frente, una nueva necesidad

La evolución tecnológica en el mundo de la información y las comunicaciones ha causado un notable cambio de paradigmas en nuestras sociedades. Cada vez es menos necesario insistir en la creciente importancia que todo lo concerniente al ciberespacio va cobrando en nuestras vidas, y cuanto veíamos hasta no hace mucho tiempo en ciertas películas de ciencia ficción forma ya parte integral de nuestro quehacer diario y es visto con la mayor naturalidad; se ha incrementado enormemente nuestra dependencia de los sistemas de información en los campos más diversos y la ciberguerra ha irrumpido con fuerza en la historia. La actividad cibernética, como toda actividad humana, presenta sus pros y sus contras; así ha ocurrido con todos los avances que han visto los tiempos: por un lado, la correcta utilización de las facilidades que nos proporcionan las nuevas tecnologías –con la consecuencia lógica de un nuevo e innegable progreso para la humanidad– y, por otro, la explotación de la capacidad de daño que también encierran –con la consiguiente necesidad que experimenta el hombre de defenderse nuevamente del propio hombre–.

Centrándonos sin más preámbulo en los aspectos de la defensa, cuando los militares nos referimos a los Ejércitos y la Armada solemos hablar de los "ámbitos y formas de acción que les son propias". Pues bien, este es un ámbito nuevo que no es propio de ninguno y lo es de todos. La historia militar ha visto cómo, en menos de un siglo, se incorporaban a los ámbitos tradicionales de la tierra y el mar otros dominios físicos: el aire y el espacio (anteayer), y uno global y artificial (en realidad, físico también): el del ciberespacio (ayer). Hoy sentimos el vértigo que nos produce constatar que es cada vez más tarde para tomar ciertas decisiones porque los acontecimientos muestran claramente que se marcha en una sola dirección.

Del mismo modo que la entrada del hombre en la tercera dimensión acabó provocando, pocos años después, la creación de fuerzas aéreas porque sin el dominio del aire las operaciones de superficie quedaban en entredicho, la entrada del hombre en el ciberespacio acabará provocando la creación de un nuevo ejército (el cibernético) cuya acción habrá que conjuntar con la de los demás, o quedaremos sorprendidos cuando las operaciones en que nos empeñemos se vean afectadas e incluso impedidas. Es más, con la aceleración general del tiempo, de que también somos testigos, no hay sino que esperar que este proceso dure mucho menos.

Aunque eso se ve aún muy lejos, efectivamente ese es el futuro, falta tan sólo una "circunstancia catalizadora" para que se haga realidad, y no resulta arriesgado afirmar que, tristemente, se tratará de un inesperado y fatídico ataque de catastróficas consecuencias (de hecho, ataques de ninguna, escasas o aún desconocidas consecuencias ya se producen a diario…). Si somos capaces de anticiparnos y reaccionar a tiempo, las consecuencias serán mínimas; si no nos organizamos antes, tarde o temprano habremos de sufrir recorriendo precipitadamente el mismo camino, pero envueltos en lamentos como hacemos cuando invertimos en blindar puertas y ventanas de nuestro hogar… dos días después de que nos hayan robado una cantidad muy superior a su importe.

Las dificultades y resistencias previsibles ante la decisión de crear un nuevo ejército son evidentes, el momento económico no es el más propicio, pero aún así se puede hacer mucho, como se indica en este dossier con el que la Revista de Aeronáutica y Astronáutica quiere hoy ilustrarnos y concienciarnos.

Pero, además, nuestra visión trasciende el mundo militar (conjunto) y el de nuestro ministerio (corporativo): entendemos la ciberdefensa como una necesidad nacional que requiere dirección unificada -a muy alto nivel- de la acción; no sólo de la contribución de las Fuerzas Armadas y aun de las Fuerzas y Cuerpos de Seguridad del Estado, sino de todos los sectores incluidos en la Ley 8/2011 sobre medidas de protección de infraestructuras críticas.

El Ejército del Aire quiere encarar con entusiasmo sus responsabilidades futuras en este ámbito, protegiendo sus sistemas de información y de armas, y sus redes de comunicación, con la información que contienen aquellos y circula por estas, compartiendo tales responsabilidades con el resto de las FAS y, según proceda, con actores no militares, para defender no sólo los sistemas y redes militares sino la nación completa.

En este trabajo, el teniente coronel López de Turiso, Jefe del Centro de Informática de Gestión (CIGES), nos aclarará conceptos e introducirá en la dimensión comunitaria (conjunta y corporativa) que necesariamente tiene la ciberdefensa. El teniente coronel Ganuza, de la División de Sistemas de Información y Comunicaciones del Estado Mayor Conjunto (DIVCIS/EMACON), incidirá en la perspectiva conjunta destacando aspectos doctrinales y de operaciones reales y ejercicios. La problemática legal y los medios actuales para defensa de la Red de Área Extensa de Propósito General del Ministerio serán abordados por el coronel del Ejército de Tierra Pérez Sanchez, Jefe del Centro de Operaciones de Seguridad (COSDEF) y, finalmente, la relación con la guerra electrónica, la situación en otros países y la perspectiva industrial serán tratados en el artículo de nuestros amigos de INDRA señores Cochrane y Coromina.

ANGEL MAZO DA PENA
Teniente General de Aviación