Las Fuerzas Armadas se preparan para afrontar con éxito los nuevos retos del siglo XXI en materia de ciberseguridad

CIBERDEFENSA militar

Capitán de navío Francisco Zea Pasquín
Jefe de la sección de Seguridad de la Información CIS
del Estado Mayor de la Defensa

La tecnología se ha convertido en un factor indispensable para el funcionamiento y futuro desarrollo de nuestra sociedad. Gracias a ella, hoy en día podemos acceder a grandes cantidades de información en tiempo y forma, independientemente de su ubicación física, desapareciendo así las barreras y fronteras tradicionales, lo que ha dado paso a la denominada Sociedad de la Información.

Del mismo modo, las Fuerzas Armadas tienen una alta dependencia de las Tecnologías de la Información y las Comunicaciones (TIC), ya que constituyen un pilar básico para poder llevar a cabo las operaciones militares. Sin embargo, este nuevo dominio donde operan estas tecnologías y que se ha venido a denominar el «Ciberespacio», está lleno de un gran número de amenazas que ponen en peligro el éxito de las operaciones militares, así como a las personas que las llevan a cabo.

Tradicionalmente, la seguridad en las TIC en el ámbito militar se ha centrado en la protección de las comunicaciones, aunque hoy en día el uso masivo de sistemas de información hace necesario disponer de una perspectiva más amplia y abordar el problema de una forma integral. De este modo surge el concepto de INFOSEC, que se basa en medidas de protección estáticas para los sistemas.

El Mando Conjunto dotará a las FAS de capacidades de defensa y respuesta

Sin embargo, la evolución de la amenaza en los sistemas CIS requiere adoptar un conjunto completo de medidas de seguridad que incluyan tanto las de carácter preventivo, como aquellas otras que aborden el carácter cambiante y asimétrico de la ciberamenaza, acción que debe llevar implícita una perspectiva dinámica que complemente la aproximación estática tradicional citada (INFOSEC). Esta aproximación dinámica, se engloba hoy en el término denominado «Ciberdefensa», que se puede definir como un conjunto de recursos, actividades, tácticas, técnicas y procedimientos para preservar la seguridad de los sistemas y la información que manejan, así como permitir la explotación y respuesta sobre los sistemas adversarios, para garantizar el libre acceso al ciberespacio y permitir el desarrollo eficaz de las operaciones militares y el uso eficiente de los recursos.

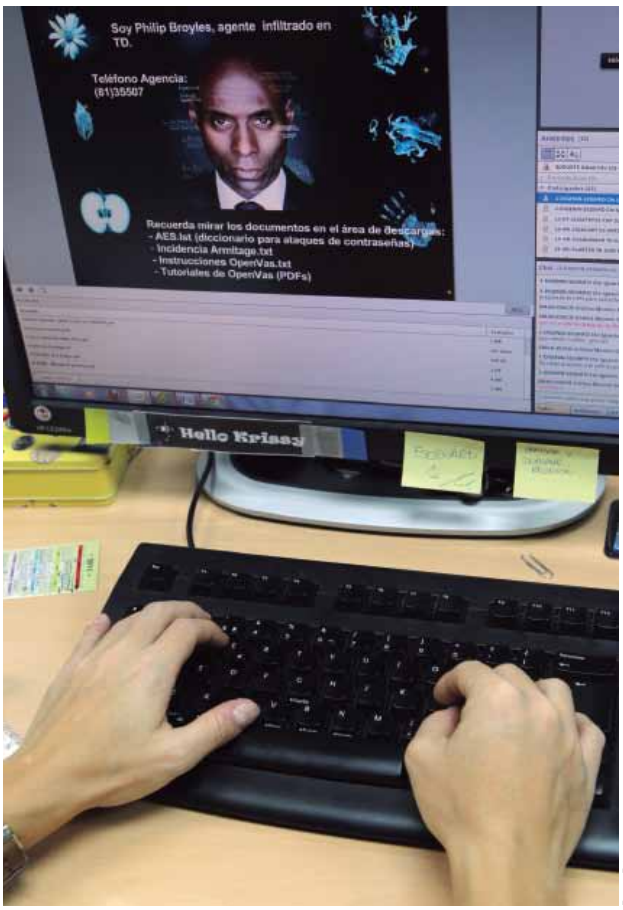
En este sentido, el Estado Mayor de la Defensa (EMAD) lleva trabajando desde hace varios años en el fortalecimiento de las iniciativas y medidas de seguridad para la protección de la información clasificada y los sistemas que la manejan. A nivel organizativo, la Sección de Seguridad de la Información CIS es la responsable de planear, coordinar y, en su caso, ejecutar las actividades de seguridad de la información en los sistemas responsabilidad del JEMAD así como la coordinación con los Ejércitos en este campo. Entre las actividades más destacadas se encuentran la ejecución de auditorías e inspecciones de seguridad para la concesión de acreditaciones, el apoyo técnico en seguridad a los distintos programas y sistemas, así como la labor de formación, concienciación y adiestramiento.

En este último aspecto, el EMAD ha venido desarrollando desde el año 2009 y con carácter anual, los denominados «Ejercicios de Ciberdefensa (ECD)», con el objetivo de adiestrar al personal del Ministerio de Defensa relacionado con la seguridad de las TIC en técnicas de protección y defensa, y en el conocimiento de aquellas otras utilizadas por los *hackers* para poder alcanzar un mayor conocimiento de cómo protegerse. En noviembre de 2012 se celebró la cuarta edición del ECD, en la que se contó con la participación de más de 30 equipos representantes de los Ejércitos y Armada, Órgano Central y Guardia Civil. Se desplegaron más de 400 máquinas virtuales y escenarios reales simulados donde los participantes, de manera remota, fueron adiestrados en diferentes técnicas de defensa y respuesta. Sin embargo, como ya se ha citado anteriormente, la Ciberdefensa va mucho más allá de unas meras medidas estáticas preventivas y debe englobar también medidas que se adapten al carácter cambiante de las amenazas y del ciberespacio. Es

por ello que el JEMAD, en diciembre de 2012, inauguró el centro de respuesta ante incidentes de las Fuerzas Armadas (CERT-FAS).

Situado en el Cuartel General del EMAD, el CERT-FAS tiene como misión la provisión de diferentes servicios de seguridad a las FAS como son: monitorización, apoyo a la resolución de incidentes, análisis forense, equipo de reacción rápida, adiestramiento, *Cyber Situational Awareness* (CSA), etc. Algunos de estos servicios, como son el adiestramiento y el apoyo a la resolución de incidentes, ya están operativos y el resto irán siendo implantados a lo largo de los próximos meses.

En esta línea, en enero de 2011 y con objeto de apoyar la definición, desarrollo y empleo de las capacidades militares necesarias que permitan garantizar la eficacia en el uso del ciberespacio en las operaciones militares, el JEMAD sanciona el documento «Visión del JEMAD de la Ciberdefensa Militar», en el cual se incluye al Ciberespacio como uno de los dominios de enfrentamiento, siendo los otros tierra, mar, aire y espacio exterior. Es en este nuevo dominio, el Ciberespacio, es donde deberán realizarse considerables esfuerzos los próximos años para dotar a las FAS de las capacidades necesarias para garantizar su libertad de acción en las operaciones militares que se desarrollen o apoyen en él. Tras la aprobación de la Visión, en julio de 2011 el JEMAD aprueba el «Concepto de la Ciberdefensa Militar» (CDM) en el que se establecen los principios, objetivos y retos de la Ciberdefensa en el ámbito militar. Asimismo, se define la terminología, se realiza una valoración de la capacidad, se presentan las funciones y responsabilidades en esta área, y se ordena la elaboración de un Plan de Acción de Ciberdefensa Militar.



Pepe Díaz

OBTENCIÓN DE CAPACIDADES

Este Plan de Acción, denominado «Plan de Acción para la obtención de la Capacidad de Ciberdefensa Militar» (PACDM) aprobado en julio de 2012, identifica las acciones necesarias para la obtención de una capacidad de Ciberdefensa Militar que cumpla con los objetivos especificados en el Concepto de Ciberdefensa Militar, como son: garantizar el libre acceso al ciberespacio con el fin de cumplir las misiones asignadas a las Fuerzas Armadas, obtener analizar y explotar la información sobre ciberataques e incidentes en las redes y sistemas de su responsabilidad, ejercer la respuesta oportuna, legítima y proporcionada ante amenazas, etc.El PACDM diseña una estrategia de obtención incremental que, empezando por una primera fase denominada Capacidad Inicial, relacionada directamente con la Capacidad de Defensa, obtiene la capacidad de resistencia ante los posibles ciberataques, así como a la recuperación de la funcionalidad de los sistemas ante los daños producidos por los mismos. Se pasará entonces a una segunda fase, denominada Capacidad Intermedia, en la que además de fortalecer la Capacidad de Defensa, se desarrollará la Capacidad de Explotación, orientada a la obtención de información sobre las capacidades de los posibles adversarios, unida a actividades de recopilación, análisis y explotación de la misma.

Por último, la tercera fase denominada Capacidad final, se centra en la obtención de la Capacidad de Respuesta ante los ciberataques que se dirijan a los sistemas CIS de las Fuerzas Armadas. Una vez obtenidas las tres Capacidades (Defensa, Explotación y Respuesta), podremos afirmar que disponemos de una Capacidad de Ciberdefensa adecuada que complementará al resto de Capacidades Militares que poseen nuestras FAS. Con el objeto de potenciar la implantación de este Plan de Acción, de manera que se haga de la forma más eficiente, el Ministro de Defensa ordena en noviembre de 2012 la creación de un Mando Conjunto de Ciberdefensa (MCCD) dependiente del JEMAD, que proporcione una unidad militar altamente especializada capaz de desarrollar y alcanzar las capacidades de Ciberdefensa descritas anteriormente. La creación del Mando se ha materializado a través de una orden ministerial publicada en el Boletín Oficial de Defensa el 26 de febrero. La normativa establece el ámbito de actuación del MCCD, que estará centrado en las redes y sistemas de información y telecomunicaciones de las Fuerzas Armadas y aquellas otras que específicamente se le encomienden.

Entre sus cometidos, destacan entre otros, el garantizar el libre acceso al ciberespacio y la disponibilidad, integridad y confidencialidad de la información y la disponibilidad e integridad de los servicios; la obtención y análisis de la información sobre ciberataques e incidentes así como ejercer una respuesta ante ellos. También desempeñará labores de dirección, coordinación, cooperación, representación y adiestramiento, siendo esta última de especial importancia ya que los miembros del mando deberán estar correctamente formados y adiestrados, tarea en la cual el EMAD, a través de los ECD descritos anteriormente, lleva tiempo trabajando, como ya se ha citado. Para finalizar, destacar que todas estas iniciativas, como son especialmente la creación del MCCD o la puesta en marcha del PACDM, permitirán dotar a la FAS españolas de las capacidades necesarias en el dominio del ciberespacio, para afrontar con éxito los nuevos retos de siglo XXI en materia de ciberseguridad. ■