Comentario THIBER:

La ciberguerra del Pentágono

AUTOR: Enrique Fojón Chamorro.
Sub-director de THIBER

A mediados de septiembre, la administración Trump publicaba la nueva estrategia nacional de ciberseguridad, una estrategia que tiene ante sí el reto de consolidar el sistema nacional de ciberseguridad estadounidense con el objetivo de preparar al país para la ciberguerra del futuro donde los ciberataques, la difusión de noticias falsas y las filtraciones interesadas tienen y tendrán un papel relevante.

En paralelo, el Pentágono ha publicado su nueva estrategia ciber, sucesora de la publicada en 2015, que deja atrás la ciberdisuasión como elemento central y propone la ciberdefensa activa como eje principal.

Durante estos últimos 3 años, el Pentágono –hasta 2016 liderado por Ash Carter- ha trabajado en la consolidación de su ciberfuerza: el U.S Cyber Command ha adquirido la condición de mando conjunto, dejando de estar subordinada a la U.S Strategic Command (USSTRATCOM), lo que conlleva que ejerza una dirección y control, en el sentido amplio, sobre las actividades en materia cibernética de los Ejércitos y la Armada; los 133 equipos que conforman la U.S Cyber Mission Force ya se encuentran operativos, lo que ha supuesto un reto de captación de talento y adiestramiento; el presupuesto del Pentágono destinado al ámbito ciber ha alcanzado los 60.000 millones de dólares; se ha prorrogado el programa de contratación de personal civil del DoD que potencia la contratación de especialistas para el desarrollo, operación y mantenimiento de las capacidades cibernéticas del Pentágono; y se han consolidado iniciativas como la Defense Innovation Unit, que comenzó como un experimento y ahora es una realidad dentro del DoD.

No cabe duda de que el Pentágono, ahora liderado por James Mattis, no conciben una operación militar, ni mucho menos la obtención de la supremacía en el campo de batalla, sin la dimensión cibernética.

Además, ciber, robótica y la Inteligencia Artificial (IA) en general se han integrado en nuevas plataformas (furtivas y no-tripuladas), sensores (C4 e ISTAR) y armas (de precisión e inteligentes) para proporcionar importantes mejoras en la forma de concebir, plantear y conducir las operaciones, permitiendo que este conjunto de sistemas puedan trabajar y operar en red y que cualquier soldado pueda conocer y controlar todo lo que sucede a su alrededor, bien sea reconociendo el terreno, identificando las amenazas, designando los objetivos o atacando los blancos en función de su situación, riesgo o disponibilidad.

En definitiva, no sólo el elemento cibernético se ha consolidado como una dimensión esencial para la optimización del planeamiento y la conducción de las operaciones en el Pentágono, sino que todos sus sistemas, armas, plataformas y procesos se fundamentan en el poder de la red para llevar a cabo sus funciones. La nueva estrategia ciber del Pentagono es un eslabon en su preparación para la ciberguerra.