Comentario THIBER:

Formar la ciberfuerza: la necesidad de integrar el dominio ciber en las operaciones militares

AUTOR: Enrique Fojón, subdirector de THIBER

Fuente: U.S. Army photo by Mike Strasser/ USMA PAO

La inmensa mayoría de nuestros socios, aliados y adversarios se encuentran inmersos en la definición y/o ejecución de los planes de adiestramiento de sus ciberfuerzas. Estos planes no solo buscan capacitar a los profesionales de la ciberseguridad y la ciberdefensa, sino deberán también servir como palanca de cambio para integrar de manera efectiva el dominio ciber en las operaciones militares.

Para llevar a cabo esta labor, buena parte de gobiernos, organismos internacionales y empresas están invirtiendo en la construcción de Cyber Ranges, una capacidad estratégica que facilita y posibilita el cumplimiento de las estrategias de ciberseguridad y ciberdefensa, esenciales para garantizar su defensa en el ciberespacio y la integración formal de la dimensión cibernética en el proceso de planeamiento de la defensa.

Un Cyber Range es una plataforma virtual que permite simular entornos operativos reales –estáticos o desplegables, clasificados o no clasificados– para la formación y el entrenamiento –individual o colectivo– de profesionales así como la experimentación, el testeo y a validación de nuevos conceptos, tecnologías, técnicas y tácticas de ciberseguridad y ciberdefensa. Para que un Cyber Range sea eficaz, deberá:

- Ser accesible en tiempo y forma por los profesionales autorizados para su utilización.

- Proporcionar un entorno seguro que permita a los usuarios ejecutar las actividades –formación, entrenamiento, experimentación, testeo y/o validación– sin poner en riesgo los sistemas en producción e información clasificada o sensible.

- Ser escalable y flexible para poder responder a las necesidades de los responsables en materia de ciberseguridad y ciberdefensa en función de la naturaleza de las actividades que lleven a cabo. No son equiparables los recursos necesarios para un curso de formación individual que para un ciber-ejercicio multinacional.

Sin embargo, la planificación de la formación de la ciberfuerza está poniendo de manifiesto la necesidad de promover profundos cambios culturales en el seno de los ministerios de defensa de nuestros socios, aliados y adversarios que posibiliten integrar a una nueva generación de ciberguerreros en una estructura organizativa y operativa que no está preparada para maximizar las ventajas que el dominio cibernético puede proporcionar.

En definitiva, la formación de la ciberfuerza no debe solo circunscribirse a un ámbito tecnológico sino también al estratégico. Los mandos militares no solo deberán comprender la importancia estratégica de las tecnologías del ciberespacio y su aplicación en la planificación y conducción de las operaciones militares, sino también deberán saber relacionarse con la industria civil para comunicar sus crecientes necesidades en el nuevo dominio cibernético.

“Los planes de adiestramiento de sus ciberfuerzas deberán también servir como palanca de cambio para integrar de manera efectiva el dominio ciber en las operaciones militares”