VICEALMIRANTE JAVIER ROCA RIVERO, COMANDANTE DEL MANDO CONJUNTO DEL CIBERESPACIO

«NUESTRO MEJOR SISTEMA DE ARMAS ES EL CEREBRO DE CADA SOLDADO»

Considera que, aunque el ámbito ciberespacial está rodeado de tecnología, lo más importante son las personas

CUANDO el pasado noviembre fue promovido a vicealmirante y nombrado Comandante del Mando Conjunto del Ciberespacio (MCCE) Javier Roca Rivero no era ajeno a los desafíos de su nuevo cargo. Durante más de tres años venía ejerciendo como segundo comandante de este Mando, responsable de asegurar la libertad de acción de las Fuerzas Armadas en el mundo digital. Sevillano de 57 años, en estos años ha adquirido un entendimiento profundo de las intrincadas necesidades que exigen las ciberoperaciones. El desarrollo del talento para seguir fortaleciendo las capacidades en este campo es uno de los retos que tiene por delante.

—¿Los militares están preparados para combatir en este nuevo campo de batalla?

—La respuesta corta es sí. Llevamos una década preparándonos para ello y tenemos suficientes capacidades para realizar ciberoperaciones, incluso integradas con operaciones convencionales. En el año 2016, en la Cumbre de Varsovia, la OTAN declaró solemnemente que el ciberespacio se convertía en el quinto ámbito de las operaciones, y que teníamos que prepararnos para operar en él y defender nuestra libertad, nuestros valores y nuestra seguridad con la misma determinación que lo hacemos en los otros cuatro ámbitos clásicos: la tierra, la mar, el aire y el espacio. España ya se había adelantado a esta visión, pues el antiguo Mando Conjunto de Ciberdefensa se creó en 2013.

—¿Las ciberoperaciones son ya relevantes en conflictos actuales, como la guerra de Ucrania?

«En los futuros conflictos sobrevivirá el que mejor se adapte y más rápido innove»

—Así es. En principio pudiera parecer que la guerra de Ucrania es una vuelta a las guerras de trincheras y artillería que asolaron Europa en el siglo pasado, pero nada más lejos de la realidad. Estamos siendo testigos de la guerra tecnológicamente más avanzada de la historia de la Humanidad, y ello es debido principalmente a la exitosa utilización en el conflicto de un nuevo ámbito de las operaciones: el ciberespacio.

Durante milenios, las guerras se libraban solo en el mundo físico y eran sangrientas, brutales, pero visibles. La guerra en Ucrania, aunque sigue siendo sangrienta, sigue siendo brutal, a menudo es invisible, al menos a los ojos de la mayoría. En Ucrania, el conflicto trascurre paralelamente en el ámbito físico y en el ciberespacial, y aunque solo podemos ver la punta del iceberg, créame que la gente real sufre y muere a consecuencia de lo que ocurre en el ciberespacio.

Los estados responsables se preparan desde hace tiempo para defenderse en un posible conflicto en este ámbito,

tratando de asegurar y garantizar su propia libertad de acción en el ciberespacio, poder acceder y operar en él, negándoselo al mismo tiempo al potencial adversario. Ucrania lo sabía, se preparó concienzudamente durante muchos años y esto ha sido clave en la supervivencia del país a la invasión rusa.

Ucrania está demostrando que en los futuros conflictos del siglo XXI no sobrevivirá el más fuerte o el más grande, sino el que mejor se adapte, el más ágil, el que mejor y más rápido innove. Por esa razón es tan importante la formación continua de nuestro personal y el espíritu de «eterno aprendiz». He leído que actualmente el conocimiento de un ingeniero queda obsoleto en diez años… Hay que renovarse continuamente y estar preparados para aprender nuevas capacidades y habilidades que ahora no existen.

—¿Qué sistemas de armas es necesario aprender a manejar para operar en el ámbito ciberespacial?

—Es importante siempre recordar que, aunque el ámbito ciberespacial parezca rodeado de tecnología, de ordenadores, de *software*… lo más importante son las personas. Y mientras más tecnología tengamos y más Inteligencia Artificial poseamos, más importantes serán las personas, sus valores, su ética en el trabajo, su compromiso y, también, su continua formación; porque en el ámbito ciberespacial, más que en cualquier otro ámbito, las capacidades residen, sobre todo, en las personas, en su aptitud y en su actitud. No tenemos grandes plataformas, aviones, buques o sistemas de armas… El arma somos nosotros. Nuestro mejor sistema de armas es el cerebro de cada soldado. Por eso, somos de las unidades que más invierten en formación de su personal.

—En la vida civil estos especialistas están muy cotizados ¿Les cuesta retener el talento?

—Aunque dedicamos nuestros mayores desvelos a fidelizar a nuestro personal (no me gusta la palabra «retener», que es un poco peyorativa y parece que tratas de engañarlo para que no se vaya), es una alegría para nosotros cuando nos dejan para un proyecto personal mejor (sea promoción interna a una escala superior o incluso en la vida civil), pues son motivo de inspiración para otros que ocuparan su lugar y es una buena manera de atraer cada vez más talento. Como dijo Henry Ford: «Solo hay algo peor que formar a tus empleados y que se vayan: No formarlos y que se queden».

—¿Cómo afrontan las Fuerzas Armadas la necesidad de especialistas en esta materia?

—Con mucha ilusión y esperanza. El Ministerio de Defensa está haciendo un enorme esfuerzo para que aquellos que lo deseen y tengan las capacidades necesarias puedan trabajar en el ámbito ciberespacial de las Fuerzas Armadas.

Existe mucha gente que se siente atraída por pertenecer a las Fuerzas Armadas y servir a España operando en el ámbito ciberespacial que, además de las unidades de ciberdefensa, incluye todo lo relacionado con las nuevas tecnologías, las telecomunicaciones, los sistemas de información, las redes de nueva generación (5G), la inteligencia artificial, la computación cuántica, etcétera.

En las recientes convocatorias para ingreso en las Fuerzas Armadas de personal cuyo primer destino será el MCCE

Entrega de diplomas del primer curso básico de Ciberoperaciones, el pasado 13 de octubre, en la nueva Escuela, encuadrada en el Mando Conjunto del Ciberespacio.

la demanda ha sido espectacular. Por ejemplo, para las 25 plazas de personal de tropa y marinería se recibieron más de 700 solicitudes, y varios centenares eran ciudadanos con estudios universitarios. Uno de los marineros que está realizando su fase de formación inicial en Ferrol y que el año que viene se incorporará al MCCE tiene tres carreras universitarias (matemáticas, informática y económicas en inglés) y, además, es investigador en IA en la Universidad Politécnica de Madrid.

El Mando Conjunto del Ciberespacio está sirviendo ahora como foco de atracción para esas personas, pero las necesidades y posibilidades incluyen todo el conjunto de las Fuerzas Armadas, pues existen unidades que realizan cometidos similares a los del MCCE en el Ejercito de Tierra, en la Armada y en el Ejército del Aire y del Espacio, donde incluso tienen ya una nueva especialidad fundamental, llamada Ciberespacio. Las Fuerzas Armadas han sido a lo largo de la Historia un referente de innovación tecnológica y ahora también es el lugar ideal para los que, además de un vida plena y entretenida, busquen una inspiración al «para qué» trabajan.

Nos queda un largo camino para alcanzar la fuerza ciberespacial necesaria para apoyar convenientemente al resto de fuerzas convencionales en el desempeño de sus misiones en un posible conflicto, pero no cabe duda de que se están dando pasos firmes, decididos y valientes en la buena dirección.

—En este sentido, ¿qué se espera de la nueva Escuela de Ciberoperaciones?

—No solo queremos formar en el plano táctico al personal que va a realizar ciberoperaciones en todas las unidades de las Fuerzas Armadas, sino que queremos enseñar también a planear y conducir este tipo de operaciones a nivel operacional, algo que no existía todavía en España.

La experiencia en algunos ciberejercicios de la OTAN nos ha enseñado que la potencia sin control no sirve de nada. No sirve de nada tener soldados muy capaces en todas las categorías y especialidades si no están bien liderados y coordinados ni existe un buen planeamiento militar inicial para ejecutar la misión. Las operaciones en el ciberespacio se deben planear y conducir igual que el resto de operaciones militares.

La Escuela de Ciberoperaciones permitirá establecer una doctrina común para las Fuerzas Armadas

Al mismo tiempo, una Escuela conjunta permitirá establecer una doctrina común para las Fuerzas Armadas y que todos sus integrantes usen no solo las mismas herramientas, sino las mismas técnicas, tácticas y procedimientos, buscando tanto la eficiencia en la gestión de recursos, como la interoperabilidad en las operaciones. Siempre digo que a un soldado herido que deba operarle un cirujano, le da igual que ese cirujano provenga del Ejército de Tierra o de la Armada; sabe que usará las mejores prácticas conocidas. Lo mismo debe ocurrir en el ámbito ciberespacial.

No nos puede ocurrir como en los inicios de la informática en el siglo pasado, donde cada ejército tomó decisiones diferentes en las herramientas que usaba y en el empleo de las nuevas tecnologías, y llegamos a tener aplicaciones diferentes para gestionar el mismo problema y sistemas de información específicos que no se «hablaban» unos con otros, pues usaban lenguajes diferentes. Los sistemas, la formación, el sostenimiento, etcétera, son muy costosos. Usar las mismas herramientas no solo permitirá que pueda haber apoyos mutuos en caso de ciberincidentes, sino que se favorece la interoperabilidad y la gestión integral de los datos y el conocimiento.

Además de estas tareas básicas, de la Escuela se espera que se convierta en un referente y una herramienta para la investigación en la aplicación de tecnologías para su empleo en todo tipo de ciberoperaciones. Deberá ser un centro que contribuya al desarrollo de doctrina nacional del ámbito ciberespacial. También creemos que una labor importante será la de establecerse como centro de referencia para la cooperación cívico-militar con empresas e instituciones educativas nacionales e internacionales.

Elena Tarilonte/Fotos: EMAD