# Compromiso individual para un uso responsable de la tecnología

**L. MARTÍN**

**CARTAGENA.** Tras la ponencia de Javier Roca, el almirante de Acción Marítima, Victoriano Gilabert Agote, fue el encargado de clausurar este nuevo encuentro del Aula de Seguridad y Fuerzas Armadas. En su intervención quiso poner en valor la «labor discreta y sigilosa, pero muy efectiva, que realizan quienes velan por nuestra ciberseguridad todos los días del año». Entre ellos, alabó la intervención del comandante del Mando Conjunto del Ciberespacio (MCCE) por «abrir los ojos hacia una realidad que no podemos ignorar», aludiendo a cómo la era digital ha mejorado la forma de vida gracias al desarrollo de las tecnologías, pero también ha abierto la puerta a «riesgos y amenazas desde un ámbito tan difícil de precisar como el ciberespacio». «No tengo ninguna duda de que debemos ser conscientes de las amenazas que allí se esconden, que nos hacen ser más vulnerables, y frente a ellas la primera línea de defensa somos cada uno de nosotros de forma individual, haciendo un uso responsable y seguro de las tecnologías digitales a nuestro alcance», dijo.

Quiso tranquilizar a los asistentes recordando que «no estamos solos», gracias a la línea de defensa que forman organismos e instituciones que protegen a los ciudadanos, incluyendo el MCCE, que «aseguran la libertad de acción de las fuerzas armadas en este espacio y que nos dan motivos para sentirnos seguros».

El Aula continuará después de verano con nuevos encuentros hasta final de año, tal y como anunciaron Gregorio Mármol y Juan Manuel Orti.

El almirante de Acción Marítima, Victoriano Gilabert, en la clausura.


▼ **Ponencia.** De izq. a dcha., Javier Roca durante su intervención, junto a Juan Manuel Orti y Gregorio Mármol.
FOTOS: **J. M. RODRÍGUEZ / AGM**

**ALGUNOS DATOS**

**90%**
**propiedad que tienen las compañías privadas del ciberespacio**

**43%**
**información que va por el ciberespacio entre máquinas**

**700**
**direcciones IP con las que puede conectar una 'smart tv' en cuestión de quince minutos**

diz», lo que supone «aprender y desaprender a gran velocidad», según el experto.

Comunicaciones

### Un mundo híbrido con nuevas amenazas

En este «mundo phygital o híbrido», como definió Roca, cambian los problemas y las preguntas, lo que hace que «no podamos combatir las amenazas del futuro con las armas y capacidades del pasado». En este aspecto, aseguró que «no podemos imaginar cómo ni contra quién combatiremos», por lo que animó a estar preparados para ver cosas nunca vistas hasta la fecha. Lo importante, apuntó, es cambiar la mentalidad, meter las nuevas ideas en la cabeza y sacar las antiguas, porque «tenemos tecnologías del siglo XXI, mentalidad del siglo XX y organizaciones del siglo XIX».

A pesar de parecer una era basada en la tecnología, el ponente transmitió que esta era va de liderazgo y de personas, de ciudadanos que en su nueva pirámide de necesidades ya incluyen tener acceso a internet y batería en sus dispositivos para estar conectados 24/7; una nueva Pirámide de Maslow en la que los valores y la ética harán que ese poder que aporta la tecnología se use para el bien o para el mal, porque «el ciberespacio es un dominio centrado en las personas y sus valores». Ahora los enfrentamientos no son con un ejército, sino con las redes sociales y todo el entorno 'online'.

«El ciberespacio no es de todos, es en un 90% propiedad de las compañías privadas que ofrecen el servicio para garantizar las comunicaciones». Roca aludió con esta información a la confianza cero, poniendo como ejemplo que «una 'smart tv' se conecta con más de 700 direcciones IP en quince minutos y oye las conversaciones».

Proteger todas las capas

### Apuesta por la ciberdefensa

En este nuevo encuentro del Aula de Seguridad y Fuerzas Armadas, Javier Roca subrayó que «el ciberespacio es otro ámbito de la vida», pero diferente al resto de elementos, porque al ser creado por el hombre para almacenar, gestionar y transportar información, puede ser modificado «a su antojo». A día de hoy, el 43% de la información que va por el ciberespacio es entre máquinas, algo que aumentará ante la evolución de la inteligencia artificial y la capacidad de éstas de comunicarse entre ellas.

Los ciberataques en este entorno tienen como característica el anonimato, lo que hace que sean fáciles los «ataques de falsa bandera», que tras una acción delictiva echan la culpa a otro, así como el bajo coste y la posibilidad de contratar capacidades. A esto se suma la inteligencia artificial, que hace que se acceda a información para cometer este tipo de delitos sin tener mucho conocimiento. Es decir, «no hace falta saber mucho para hacer mucho daño». «En España hay talento, pero se está usando, cada vez más, para hacer el mal», aseguró el ponente.

Eso hace que este entorno asimétrico y con actores privados se arbitre por «la ley del más fuerte», donde la amenaza puede aparecer desde cualquier lugar y sin alerta previa. El problema es que «en el ciberespacio es más fácil atacar que defenderse». «Los malos solo temen al fracaso, porque con acertar una vez ya te comprometen el sistema, y el eslabón más débil siempre son y serán las personas», indicó Roca.

**«Lo más característico de esta era digital es la hiperconectividad y la aceleración»**

**«No podemos combatir las amenazas del futuro con las armas y capacidades del pasado»**

**«Somos testigos de la mayor transformación de la historia de la humanidad»**

Los ataques más probables son hackeos del ordenador, que bloquean toda la información y piden un rescate para aportar las claves. A pesar de que lo más peligroso parece centrarse en las tecnologías de la información (IT), para Roca está en la tecnología operativa (OT), que engloba las tecnologías y sistemas, como el hardware y software que supervisa y controla los procesos y máquinas en el ámbito industrial y que los ingenieros deben proteger a nivel tecnológico. También recordó la existencia de APT (Amenaza Persistente Avanzada), grupos de miles de personas que trabajan todos los días para comprometer sistemas y países y que se despliegan en diferentes lugares del mundo.

Ante esto, señaló la apuesta por la ciberseguridad para defender todas las capas que puedan presentar vulnerabilidades, además de la ciberdefensa, que no solo protege las redes y la información, sino que defiende los derechos y libertades, la paz y la seguridad. «Las fuerzas armadas dependen permanentemente del ciberespacio y la vulnerabilidad de este ciberespacio es la mayor amenaza a la seguridad nacional de origen humano por probabilidad de que ocurra un suceso y por el impacto que tendría, mayor que el crimen organizado, un conflicto armado o una pandemia», aseguró. A pesar de esto, el ponente animó a «ser optimistas y pensar que vamos a ganar esta guerra», confiando en las herramientas de ciberdefensa nacionales y en los profesionales que dedican sus esfuerzos a este fin, incluyendo la labor de conjunta con las universidades, como es el caso de la Politécnica de Cartagena a través del Trust Lab, cuya directora, María Dolores Cano, junto a parte su equipo, estuvieron presentes en el encuentro.