El Ejército del Aire frente a la COVID-19. ¿Y ahora qué?

Miguel Castro Arjona
Capitán del Ejército del Aire

Aventurar el futuro es siempre un ejercicio de riesgo equiparable a estar sobre un cable a 50 metros del suelo, más aún en tiempos de gran incertidumbre como los que vivimos.

Y, sin embargo, mirar al futuro es una exigencia profesional y anímica que forma parte de nuestro ADN tal y como reflejan estos versos de nuestro himno: «Alcemos el vuelo», «La esperanza nos lleva detrás», «Tenaz el empeño», «Jamás bajaremos desde nuestro sueño», versos que reflejan con precisión este espíritu de superación. Un afán que nos impulsa constantemente a adaptarnos, a superar las dificultades, a elevarnos sobre los problemas y las limitaciones que nos impone nuestro entorno para mirar más allá del horizonte.

Por ello, cuando empezamos a recobrar el aliento después de duras semanas de lucha desigual contra un enemigo invisible, es tiempo de empezar a pensar en el futuro que tenemos que enfrentar y cómo adaptarnos a él para mantener nuestras capacidades y misiones durante el tiempo en que tengamos que convivir con la actual amenaza biológica.

En tanto no se disponga de la anhelada profilaxis que nos permita recuperar la normalidad, hay que asumir las limitaciones que supone operar con una adecuada asepsia que garantice la salud de nuestras tripulaciones y que no por necesaria deja de ser engorrosa.

El mantenimiento de la distancia de seguridad interpersonal, la disponibilidad de equipos de protección personal y de los medios de

desinfección condiciona, cuando no limita, el mantenimiento y recuperación de aeronaves y, con ello, las misiones encomendadas al EA tanto en territorio nacional como fuera de él. Otro tanto afecta a las labores de instrucción y docencia.

Finalmente, y al igual que para el resto de organismos públicos y privados, la concentración de unidades y mandos en torno a grandes urbes supone un reto adicional por cuanto el personal que integra estas unidades tiene que sortear las dificultades ya mencionadas, sumando las que la emergencia sanitaria añade a la vida cotidiana en las grandes urbes, como son desplazamientos colectivos, limitación de aforos, distancia de seguridad, etc; y todo ello con el añadido de tener que conciliar la vida familiar en un momento en que los colegios y muchas empresas han cerrado.

Con este panorama, decir que el futuro pasa por apoyarse en las tecnologías de la información (TIC) puede parecer una perogrullada, ¿pero lo es? Afortunadamente, hace años que los grandes proveedores de servicios de telecomunicación nacionales respondieron a esta cuestión invirtiendo en desplegar una gran infraestructura de fibra que está sustentándonos en estos tiempos difíciles.

A pesar de ello, mis años de servicio en esta querida institución me han enseñado que nunca falta quien se cuestione qué tiene que ver el desarrollo de las TIC con las misiones de las alas de caza, transporte y helicópteros que constituyen el pilar fundamental del poder aéreo.

Para explicarlo, en mis años de docencia solía recurrir al símil del iceberg, del que, como es bien sabido, solo aflora una décima parte que, sustentada por la flotabilidad del resto, se yergue desafiando a la inmensidad de los océanos.

Tirando de doctrina, la esencia de cualquier fuerza aérea no es otra que la de desarrollar el vuelo en todas sus facetas, garantizando el uso de la dimensión aérea en todo momento para, desde ahí, proyectar y extender su acción al resto de dimensiones.

Pero para ello, al igual que el iceberg precisa de una gran masa que lo sustente y mantenga a flote, las actividades aéreas precisan de una ingente cantidad de procesos y acciones previas que proporcionen los medios, el personal, las instalaciones y los servicios necesarios para desarrollarlas con seguridad y eficacia.

Por ello, aligerar el volumen de la base de sustentación con tecnología no es cuestión baladí en tiempos como los que se avecinan.

Y es que, en estos aciagos días, las telecomunicaciones están desarro-

llando un papel indispensable para poder mantener los servicios e instituciones del Estado que sustentan nuestra sociedad, y no digamos para sobrellevar la anomalía social que supone para un país acostumbrado a vivir en la calle verse forzado a un largo confinamiento en nuestros domicilios.

Desde la acción del Gobierno hasta el ocio, pasando por la cesta de la compra o la educación, todos los sectores y actividades se han visto abocados a migrar a la dimensión cibernética para poder sobrevivir en estos tiempos. Así, teletrabajo, *co-working*, videoconferencia, han pasado a formar parte de nuestro léxico diario.

Sin embargo, el incremento exponencial del uso de la infraestructura de telecomunicaciones ha puesto de relieve varias circunstancias:

– Aunque muy avanzado, el despliegue tecnológico es aún muy desigual, y otro tanto ocurre con la implantación de la identidad digital, lo que dificulta la aplicación y seguimiento de procesos con soporte digital, ya sea administrativos, educativos o de gestión, avocándonos a interrumpirlos.

– El amplio desarrollo y despliegue de soluciones ofimáticas, *apps* y sistemas de información que transitan por internet, conforman un amplio ecosistema de aplicaciones que consumen una ingente cantidad de recursos y han puesto nuestra infraestructura de telecomunicaciones al límite de su capacidad.

– La concentración de infraestructuras y servicios en grandes urbes supone un reto adicional en la continuidad de los mismos, ya que las bajas por contagios, la movilidad y la conciliación de las personas encargadas de mantenerlos son un importante hándicap que condiciona su continuidad cuando no se disponen de medios para teletrabajar.

– Finalmente, esta migración abrupta al mundo digital ha supuesto un incremento en la exposición a los ataques cibernéticos a infraestructuras y dispositivos, tanto oficiales como particulares, que convierten al mundo digital en un caldo de cultivo para la proliferación de virus y *malware* que comprometen nuestra seguridad y la integridad de nuestros sistemas.

En un escenario económico poco favorable, no parece probable que se pueda ampliar las ya mermadas plantillas orgánicas, y no hablemos de ampliar partidas presupuestarias para infraestructuras, movilidad, etc., lo que nos aboca a tener que optimizar al máximo los recursos actualmente disponibles y, especialmente, la infraestructura tecnológica.

Esto va a requerir de metodología y disciplina para evitar que en lugar de reducir el trabajo, este se multiplique, saturando las redes y convirtiéndolas en una torre de Babel como ocurre con los grupos de WhatsApp que el común de los mortales «sufre» en más de una ocasión.

Tanto la mensajería instantánea como la convencional ofrecen un entorno ágil y accesible que facilita la comunicación a distancia, tan importante en estos días, permitiendo la transmisión de órdenes y novedades, así como multitud de gestiones.

Pero está demostrado que su uso requiere de disciplina y coordinación, ya que, en caso contrario, es un caldo de cultivo para convertirse en la ingobernable torre de Babel que he citado anteriormente.

Ejemplos de buen uso los podemos encontrar en salas de mando y control como las disponibles en el Sistema de Defensa Aérea, BOCS/WOCS y el JFAC, que utilizan exitosamente estas tecnologías mediante la identificación y jerarquización de los actores que intervienen en cada sala, una fraseología común, unos procedimientos y metodologías de trabajo bien definidas.

El uso coordinado de ambas herramientas consigue reducir tiempos, facilitando el control y permitiendo configurar una SA rápida y dinámica, que posibilita al mando una adecuada comprensión del estatus de sus unidades a la par que un canal de transmisión inmediata de sus órdenes.

Aunque cada vez son más los procesos que se centralizan mediante aplicaciones de uso e interfaz común, aún existen infinidad de procesos cotidianos que, desde los mandos, descienden a diario hacia las unidades solicitando información sobre personal, formación, material, etc. Dicha información debe luego ser recibida en cada estado mayor para armonizarla, fusionarla y priorizarla de cara a la toma de decisiones.

Disponer de un repositorio o interfaz común donde cada unidad pudiese aportar su información para que esta sea automatizada y debidamente procesada reduciría en gran medida el tiempo y el esfuerzo que actualmente tienen que emplear los mandos para gestionar sus respectivos recursos.

Haciendo para nuestra organización una abstracción de las tendencias en gestión usadas en el mundo empresarial, se trataría de cambiar el actual paradigma *push*, en que las tareas se reparten en sentido descendente, al *pull*, en que cada actor se encarga de proporcionar sus productos en los tiempos y repositorios indicados.

Un buen ejemplo de este paradigma es el SIUCOM (Sistema de Información de Unidades Centros y Mandos). Del análisis de una situación en que cada unidad aérea, y según su peculiar idiosincrasia, configuraba unas inmensas tablas Excell, cuyos datos resultaban difíciles de aunar dada la disparidad de formatos e interpretaciones, provocaba en no pocas ocasiones una distorsión de la visión que se le ofrecía al mando sobre estatus situacional de sus unidades aéreas.

El problema reside en que el SIUCOM, como el SIPERDEF, SL-2000, SIMENDEF, SIDAE y tantas otras soluciones de gestión, se han ido desarrollando de forma independiente y actualmente conforman un ecosistema deslavazado y de uso desigual, que impide el uso de tecnologías de gestión avanzadas como las de *big data*, que tan útiles se han mostrado para la identificación y optimización de procesos y recursos de grandes organizaciones como la nuestra.

Esto, unido a los diferentes niveles de seguridad vigentes para cada sistema, redunda en la multiplicidad de redes y terminales que se conectan a las mismas, en una dispersión y duplicidad de la información, lo que en no pocas ocasiones resulta en una inconsistencia de la misma, forzándonos a tener que hacer continuos reajustes o a multiplicar el trabajo para introducir la misma información en varios sistemas de información.

Por tanto, hacer un esfuerzo de integración y simplificación redundará en aligerar de forma considerable la panza de nuestro iceberg, explotando al máximo la ingente cantidad de datos de que actualmente disponemos, mejorando en la gestión de los recursos de material y personal con que nos dote el Estado para ofrecer a los mandos información rápida y consistente que les ayude en su gestión.

No por difícil es menos necesario unificar a las diferentes autoridades operacionales sobre los criterios de uso de sus respectivos sistemas/da-

tos, porque sin duda es un paso indispensable si se quiere conseguir una gestión optimizada de nuestra infraestructura de telecomunicaciones, al menos mientras no se consigan recursos para ampliarla.

Afortunadamente, el EA lleva ya tiempo incrementando las promociones de personal con perfiles CIS, profesionales que serán los llamados para poder acometer esta tarea de análisis, diseño y explotación de nuestros medios CIS.

También se ha trabajado en ampliar y segmentar las redes (propósito general y mando y control) para securizarlas y desplegarlas por nuestras unidades y agrupaciones aerotácticas de la mano del desarrollo de las comunicaciones satelitales.

Porque si algo nos está enseñando esta situación es que el futuro pasa por la tecnificación y la desglobalización, ya que el mayor enemigo de los virus, biológicos o tecnológicos, es la dispersión.

Dispersión y trabajo colaborativo requieren, como ya he dicho, de metodología y disciplina en el uso de los medios telemáticos, pero también de telegestión y, por ende, de seguridad y resiliencia.

Esta es la esencia del paradigma «dirección centralizada y ejecución descentralizada» que se impone en la actualidad; identificar, coordinar y aprovechar los recursos y el talento allá donde se encuentren y que ha tenido un rotundo éxito en iniciativas como la conocida comunidad CoronaMakers, que ha sido capaz de diseñar, fabricar y repartir ingentes cantidades de material indispensable para afrontar la crisis de la COVID-19.

De igual manera, dirigidos desde la JSTCIS y sus unidades específicas, el personal CIS que está distribuido por todas nuestras unidades podría jugar un papel esencial en el futuro para poder colaborar en esta tarea unificadora e innovadora.

Ya sea colaborando en el análisis y optimización de las redes, procesos y recursos de cada unidad, o incluso aprovechando las posibilidades telemáticas de que disponemos, dicho personal podría integrarse en equipos de desarrollo y explotación que proyecten y multipliquen las capacidades de la Jefatura CIS.

Así podríamos contar, allá donde se encuentre, con todo el talento de que disponemos, en lugar de forzar a dicho personal a elegir entre vocación o conciliación familiar, lo que actualmente nos está privando de muchas manos indispensables en tiempos de carestía.

Por otra parte, y en unos momentos en que hay una lucha atroz por captar talento con dichos perfiles, las Fuerzas Armadas no podremos competir en términos económicos con la empresa privada, lo que nos obligará a un esfuerzo continuo en formación que no se verá debidamente recompensando con una mayor eficiencia en nuestra infraestructura CIS.

Por el contrario, contar con dicho personal supondría:

- Un estímulo que nos permitiría competir en términos de «salario emocional», fidelizando a nuestros

técnicos, que ya no se verían en la disyuntiva de elegir vocación o conciliación.

• Favorecer la deslocalización de nuestra fuerza crítica en aras de ganar en resiliencia ante emergencias como la actual.

Como ya he mencionado, la complejidad y sensibilidad de los datos que se manejan en el entorno del Ministerio de Defensa, introducen un factor de complejidad que dificulta el teletrabajo y la integración de sistemas.

Afortunadamente, contamos con la inestimable ayuda del Mando Conjunto de Ciberdefensa que, junto con el CCN[1] e Incibe[2], están demostrando cómo, fruto de compartir información y experiencias de sus respectivos CERT[3], se pueden editar guías de configuraciones seguras para dispositivos y redes que ayuden a reducir el perímetro de riesgo para superar los problemas de seguridad en el acceso remoto.

En resumen, debemos avanzar sin demora en la transición a la dimensión analógica desde el convencimiento de que es y será una apuesta segura en la que invertir esfuerzos y recursos.

Simplificar los procesos administrativos, integrar sistemas de información para sacarles el máximo partido, disgregar y redundar las infraestructuras TIC para favorecer teletrabajo y resiliencia, repartir el esfuerzo técnico en el desarrollo y mantenimiento de nuestro tejido CIS para aprovechar todo nuestro talento actualmente disperso y culminar el proceso de despliegue de dispositivos de identidad digital que nos permita habilitar un acceso seguro a nuestra infraestructura de comunicaciones que garantice, no solo la continuidad de los procesos administrativos y logísticos necesarios en nuestro día a día, sino un acceso confiable a los diferentes sistemas de información que sustentan el planeamiento y conducción de nuestras operaciones y el imprescindible mando y control de nuestras unidades.

Por tanto, avanzar en el uso y control de la dimensión cibernética no solo es preciso para prevalecer en nuestra nativa dimensión aeroespacial en unos escenarios híbridos tan inciertos y complejos como el que afrontamos actualmente, es además una buena forma de innovar en tiempos difíciles y una apuesta segura de cara a dominar los escenarios del futuro. ■

NOTAS

[1]CCN: Centro Criptológico Nacional (la cabeza de la ciberdefensa nacional y responsable de la parte institucional).
[2]Incibe: Instituto Nacional de Ciberdefensa (la parte de la ciberdefensa para el ámbito civil y empresa).
[3]CERT: *computer emergency response team* o centro de respuesta a emergencias informáticas. Cada uno de los tres organismos anteriores tiene el suyo que, junto con los que montan las grandes empresas, conforman la red de centros CERT nacional.