Las telecomunicaciones tácticas militares: vanguardia de la transformación digital del campo de batalla

Salvador Llopis Sánchez
Academia de las Ciencias y las Artes Militares
Sección de Prospectiva de la Tecnología Militar

26 de septiembre de 2021

El entorno de las telecomunicaciones tácticas militares.

Si por algo podría caracterizarse el entorno de las telecomunicaciones tácticas militares es por ofrecer oportunidades a una amplia variedad de tecnologías emergentes que podrían suponer grandes cambios en la doctrina y en cómo se desarrolla el ritmo de las operaciones. El nivel táctico de las operaciones es "donde la misión tiene lugar" y por ese mismo motivo es el campo de la ciencia y arte militar donde se exige una mayor dedicación a la hora de aportar soluciones que faciliten al combatiente o a las pequeñas unidades terrestres, marítimas, aéreas o del ciberespacio su función. Esta dedicación viene motivada por la prueba de su utilidad en situaciones muy concretas de gran sobrecarga del espectro electromagnético y de la presencia de multitud de fuentes de información y sensores. Se habla del nivel táctico para referirse al último eslabón de una estructura de mando jerarquizada donde el nivel operacional y el estratégico son respectivamente sus escalones superiores.

Las tecnologías emergentes a las que se debe prestar atención en el entono táctico comprenden principalmente: (1) la radio definida por software y su extensión a redes definidas por software, (2) el estándar 5G para las comunicaciones móviles inalámbricas debido a la sustancial mejora de las prestaciones, (3) la computación en la nube, (4) el uso extensivo de las comunicaciones satélite civiles y militares y finalmente (5) el procesamiento y fusión de la información disponible por medio del uso de la inteligencia artificial.

La importancia del nivel táctico con respecto a los demás niveles de mando – operacional y estratégico – radica en constituirse la frontera de la red, de su carácter eminentemente dinámico y ser asimismo los 'ojos' donde visualizar la situación en proximidad del adversario. Para cumplir con esta misión, el nivel táctico debe dotarse de unas telecomunicaciones de vanguardia para su uso aún en ambientes

con alta congestión electromagnética o degradados que pudieran impedir utilizar todas las prestaciones de los medios disponibles. A nivel táctico es primordial poder sacar todo el provecho a las tecnologías emergentes citadas.

Los desafíos existentes a la hora de incorporar nuevas funcionalidades a las telecomunicaciones tácticas pueden verse fundamentalmente desde dos prismas. El primero de ellos es la componente de red o telemática donde prima la arquitectura de la solución y su infraestructura en una red federada de misión. El segundo se centra en la integración de los elementos externos a la red o componente de señal. Aunque ambos prismas pueden considerarse indivisibles del punto de vista práctico, la principal utilidad de esta visión es de carácter técnico. Permite abordar la división de tareas de los dispositivos de red permanentemente conectados y de aquellos otros que se conectan o desconectan de una forma dinámica a la red como los sensores, cualquier fuente de información heterogénea y los equipos terminales de usuario que generan e intercambian información. Esta división prevalece en los diferentes niveles de mando, aunque el entorno táctico se caracteriza por un mayor uso de la componente de señal.

La transformación digital no está exenta de dificultades a la hora de establecer un balance entre las mejoras a obtener con el despliegue de medios dotados de nuevas tecnologías y la supervivencia de los sistemas existentes con los que se debe buscar un cierto grado de interoperabilidad. La modernización de las telecomunicaciones tácticas debe atender a criterios operativos de la fuerza que participa en operaciones; como su preparación y su nivel de disponibilidad. En aras de fomentar la innovación y aproximar soluciones que pudieran ser desplegadas rápidamente en operaciones, los procedimientos deben estar correctamente concebidos para facilitar una investigación básica que pudiera avanzar hacia prototipos avanzados.

Cambios de paradigmas en la modernización de la capacidad de red.

Suele referirse a un paradigma cuando existe un modelo de conocimiento científico comúnmente aceptado. Es muy probable que la drástica introducción de las tecnologías emergentes como el big data, las redes definidas por software o la inteligencia artificial provoquen cambios en varias áreas de conocimiento y en sus técnicas. No hay duda de que las futuras tecnologías a implementar en las telecomunicaciones tácticas proporcionarán un mayor flujo de información al combatiente desplegado en misiones. La información recibida deberá ser procesada de forma inteligente para que se identifique automáticamente aquella que se considere critica para la toma de decisiones en tiempo oportuno. La dependencia de estas tecnologías emergentes con respecto al software es cada vez mayor, lo que refuerza la importancia de dedicar más esfuerzos a las técnicas

de desarrollo de software seguro y eficiente. El cambio a experimentar vendrá motivado por dar un mayor protagonismo al software. Otro cambio vendrá motivado por la deslocalización de la información y su almacenamiento en nubes de computación tácticas lo que puede provocar que las redes sean muy descentralizadas; abandonando la idea de una estructura jerárquica basada en niveles de mando. O incluso podrían surgir nuevas topologías de infraestructura de red más dinámicas, autónomas e innovadoras. El modo en que el nivel táctico y sus telecomunicaciones se adapten a las nuevas circunstancias del combate influirá en la selección de las tecnologías que deban soportar los escalones de mando superiores para ser interoperables.

La ventaja en cualquier conflicto no vendrá dada únicamente por el número de efectivos de la fuerza a emplear o sus medios, sino por la capacidad de obtener una superioridad de la información; lo que implicaría fomentar un diseño de sistemas de telecomunicaciones que empleen arquitecturas abiertas y de carácter modular - en una especie de *plug and play* de componentes que permita sustituir o actualizar módulos del sistema cuando sea necesario sobre un núcleo común – y un desarrollo ágil del software en constante interacción con el usuario final para verificar que se cumplen los requisitos esperados. Esa misma puesta en práctica de metodologías ágiles reducirían el *time-to-marke*t de los desarrollos y por tanto su despliegue en misiones. Dada la velocidad a la que se esperan las posibles actualizaciones de los sistemas de información, es fundamental establecer un

procedimiento de control de la configuración en línea con el predominio del software mencionado anteriormente.

Siendo conscientes de que las tecnologías de uso dual –aquellas que surgen en el ámbito civil y que pueden derivar un uso militar– primarán en gran medida las iniciativas para dotar a las fuerzas armadas de tecnologías punteras. Esto significaría aprovechar la oportunidad de usar tecnologías comerciales que pudieran satisfacer casos de uso en el contexto militar.

Hacia una red táctica integrada para el combate colaborativo.

El combate colaborativo es una aproximación conceptual reciente que nace de otras iniciativas en el campo de los sistemas de mando y control multidominio. Esta forma de combate resalta las características de una completa integración, en el ámbito conjunto, de plataformas, fuerzas, terminales de usuario y cualquier otra fuente de información con el objetivo de contribuir a una rápida toma de decisiones y a un conocimiento compartido de la situación. Esta colaboración implícita exige una interconectividad sin precedentes que no tiene por qué estar centrada en una única infraestructura de red. El combate colaborativo esta potenciado por el uso de tecnologías emergentes como la inteligencia artificial, el big data, el internet de las cosas, la computación en la nube o los sistemas autónomos. Los primeros intentos de destacar la importancia de una conectividad de red que permitiera compartir información en un campo de batalla digital y conjunto surgen con la guerra centrada en la red –en la que la potencia de combate generada del enlace efectivo de todas las fuerzas en una zona de operaciones sirve para crear un conocimiento compartido del espacio de batalla– y a la capacidad para operar en la red que analiza las consecuencias de disponer de una infraestructura de red usada como medio para conectar diversos nodos de información o puestos de mando. Estos últimos conceptos parecen estar en desuso en el momento actual en que la conectividad total alcanza su mayor expresión en redes de telecomunicaciones multipropósito, ya sean inalámbricas, usando medios radio o satélite, o de carácter ad-hoc, móvil o permanente.

La pregunta que cabe hacerse es cómo obtener una red táctica integrada que cumpla con los requisitos a establecer para el combate colaborativo. La computación en la nube puede constituir gran parte de la respuesta ya que permite obtener mayor capacidad de proceso computacional que con recursos tradicionales, además del acceso a aplicaciones y almacenamiento masivo de datos, prescindiendo de la necesidad de realizar grandes inversiones en hardware. La implantación de una cultura de computación en la nube y especialmente en el nivel táctico, no está exenta de retos, aunque también de oportunidades. El camino a seguir ya está siendo explorado por programas como la *Joint Enterprise Defence*

Initiative (JEDI) del Departamento de Defensa de EEUU o el *Nexium Defence Cloud* seleccionado por la OTAN. El disponer de un entorno informático moderno que sea capaz de actualizarse al ritmo que progresa la tecnología y que proporcione un acceso seguro, deslocalizado y con alta disponibilidad a centros de datos, es de por sí una evolución considerable. La gestión de la información táctica a compartir transcurriría de esta forma desde las capas más periféricas o *tactical edge* donde se ubican los medios aéreos, navales o terrestres que realizan la misión conjunta hasta la capa que comprende los nodos de computación en la nube táctica.

Entre ambas capas la conectividad debe estar asegurada y ahí es donde, tanto las comunicaciones móviles inalámbricas de quinta generación o 5G como las comunicaciones satélites permitirán una mayor resiliencia del entorno táctico poniendo el foco en la disponibilidad y en la gestión eficiente del espectro electromagnético. El progreso no acaba aquí pues ya se está trabajando en comunicaciones móviles 6G previstas para antes del año 2030 y en las aplicaciones que podría ofrecer una constelación de satélites de órbita baja, de baja latencia (referida al retardo temporal que existe en el procesamiento de la información debido a la distancia y a las condiciones de propagación de la señal) y de banda ancha de alta velocidad como Starlink de Space X para su empleo en el entorno táctico. Starlink es una red de más de mil satélites con el objetivo de alcanzar una cobertura global terrestre y servicios de conexión ultrarrápida a internet con datos estimados en el enlace de bajada de entre 50 y 150 Mbps. Se espera que las prestaciones pudieran ser mejores conforme la red se vaya ampliando y consolidando su arquitectura. El impulso actual a las comunicaciones satélite también viene dado por el sistema de conectividad seguro basado en el espacio, una iniciativa de la Unión Europea para futuras conexiones seguras digitales considerado como un tercer pilar de infraestructura espacial junto a los programas Galileo y Copernicus. Este proyecto está inicialmente diseñado como una iniciativa de satélites multi-órbita (tanto de órbita baja como geoestacionaria) permitiendo también la realización de comunicaciones cuánticas seguras.

Las comunicaciones vía radio seguirán ofreciendo un enlace principal y seguro que es necesario preservar dada su importancia operativa, todo ello con independencia de las mejoras de las comunicaciones satélite en el entorno táctico. En este sentido, la radio definida por software permite compatibilizar un mismo equipo radio con portabilidad para diferentes formas de onda siendo capaz de integrarse en redes definidas por software, las cuales separan el control de la red de las aplicaciones. Esta flexibilidad las convierte en más sencillas de reconfigurar cuando existe una alta movilidad de usuarios. Estos avances deben estar íntimamente ligados a obtener una mejora de las capacidades de ciberdefensa en sintonía con las posibles vulnerabilidades que pudieran surgir.

Uno de los conceptos emergentes en el diseño de las telecomunicaciones tácticas trata el estudio de los «sistemas de confianza cero». El principio de confianza cero considera que ningún usuario de la red pueda disponer de garantías implícitas para acceder sin que medie un exhaustivo control. Se trata de una medida de seguridad que busca proteger los recursos y no los segmentos de la red táctica, ya que su perímetro se extiende más allá de un entorno propio local. De esta forma, la seguridad se aplica a todos por igual independientemente de su ubicación física. Tanto los usuarios locales como los remotos deberán pasar por un proceso riguroso de autenticación para poder acceder a los servicios. Este modelo puede ser de utilidad para proporcionar resiliencia -entendida como resistencia dinámica frente a incidentes- a una compleja topología de la red táctica con multitud de nodos de información. Uno de los condicionantes será comprobar que estas medidas no afectan sustancialmente al rendimiento esperado de la red. La premisa es asumir que la red se pudiera encontrar comprometida por lo que es necesario monitorizar en todo momento su estado. Este sistema avanzado de seguridad se aplica a todos los recursos de la red, tanto a máquinas como a las aplicaciones software que deben autenticarse en cada transacción. El análisis y evaluación de los riesgos lleva a considerar que se establezcan mínimos privilegios de acceso para cualquier usuario, procediéndose a realizar una diagnosis completa de esa confianza con cada transacción o sesión. Para redes de gran escala, la confianza cero significa evolucionar las técnicas de ciberdefensa clásicas basadas en la protección del perímetro de la red y en los interfaces de conexión a un modelo que se ajuste a un gran dinamismo en los flujos de datos y a la necesidad de configurar una mayor granularidad en la arquitectura de seguridad. Con este propósito, el dispositivo que vela por el cumplimiento de las políticas de seguridad se apoya en elementos avanzados de decisión como algoritmos de confianza que permitan obtener una autenticación y autorización eficaz de los usuarios.

Vislumbrando oportunidades en futuros desarrollos.

Para completar una visión de futuro en el área de las telecomunicaciones tácticas, cabe resaltar los avances relativos al diseño de centros de operaciones y puesto de mando cognitivos o de nueva generación. El procesamiento automático de los datos, las nuevas técnicas de visualización con realidad virtual o aumentada unidas al uso de la inteligencia artificial potenciarán los centros de operaciones actuales para reducir los tiempos en la toma de decisiones de un campo de batalla digital que se espera acelere el tiempo en el que se suceden las acciones para el cumplimiento de las misiones. Las soluciones para lograr un conocimiento de la situación -entendido como la capacidad de comprender lo que está sucediendo en varios dominios operacionales (terrestre, marítimo, aéreo y del ciberespacio) al mismo tiempo- guiarán la transformación digital de dichas estructuras de mando para maximizar los factores cognitivos del ser humano (percepción, razonamiento,

atención, etc.) en aras de alcanzar una ventaja en la decisión. Esta ventaja consiste en romper el ciclo de decisión del adversario, adelantándose y privándole de libertad de acción.

Muchos de los futuros desarrollos buscarán aproximar la mejor arquitectura posible de telecomunicaciones en el nivel táctico de una forma gradual. Esto significa modernizar los medios de integración (enrutamiento y procesamiento de la información) para que coexistan tecnologías heredadas con otras nuevas que se encuentren listas para desplegarse en operaciones. La red de telecomunicaciones deberá ser flexible, autoconfigurable en mayor medida, escalable, interoperable y permitir la alta movilidad de los elementos a conectar. Además, será conceptualmente diseñada como un «sistema de sistemas» o «burbuja de nodos de acceso interconectados» relanzando la importancia de aplicar una rigurosa metodología de ingeniería de sistemas que auxilie en las tareas de diseño, planificación y mejora. En este desafío está la esencia del éxito para lograr el soporte de telecomunicaciones que requiere un sistema de mando y control conjunto y multidominio en un entorno de hiperconectividad como el descrito.