El papel de la tecnología avanzada en una base inteligente

Documento técnico

Alcatel·Lucent
Enterprise

Índice

"Los datos siempre han contribuido al éxito en Defensa y se están convirtiendo rápidamente en nuestra razón de ser. Cada decisión que tomamos se basa cada vez más en los datos: desde inversiones y desinversiones multimillonarias hasta situaciones de vida o muerte que se resuelven en una fracción de segundo en el campo de batalla, pasando por la defensa frente al creciente volumen de ciberamenazas... A pesar del creciente volumen de datos procedentes de un arsenal cada vez mayor de sensores, nos resulta más difícil que nunca aislar la señal del ruido. Es la paradoja de los datos de Defensa."[1]

MINISTERIO DE DEFENSA DEL REINO UNIDO

Introducción

Cuando se trata de tecnología avanzada, el sector de la defensa es bien conocido por su sofisticación. Las organizaciones de defensa de todo el mundo, ya sean de desarrollo propio o comercial, están adoptando y adaptando enérgicamente tecnologías para su aplicación en escenarios de combate y guerra. Además, cada vez más, el motor de su estrategia es la adquisición, distribución o gestión de datos.

Esto se debe no solo al enorme volumen de datos –que experimenta un crecimiento anual de dos dígitos–, sino también a la naturaleza del panorama de las amenazas, que ahora es mucho más complicado por la necesidad de vigilar y abordar constantemente el problema emergente de la ciberdelincuencia y la desinformación.

Aquí es donde es fundamental una estrategia de transformación digital. Aprovechando las tecnologías de la información y la comunicación (TIC) para conectarlo todo, en todas partes, el sector puede aprovechar más plenamente los datos disponibles y moverlos de forma más eficiente y segura dentro de sus organizaciones.

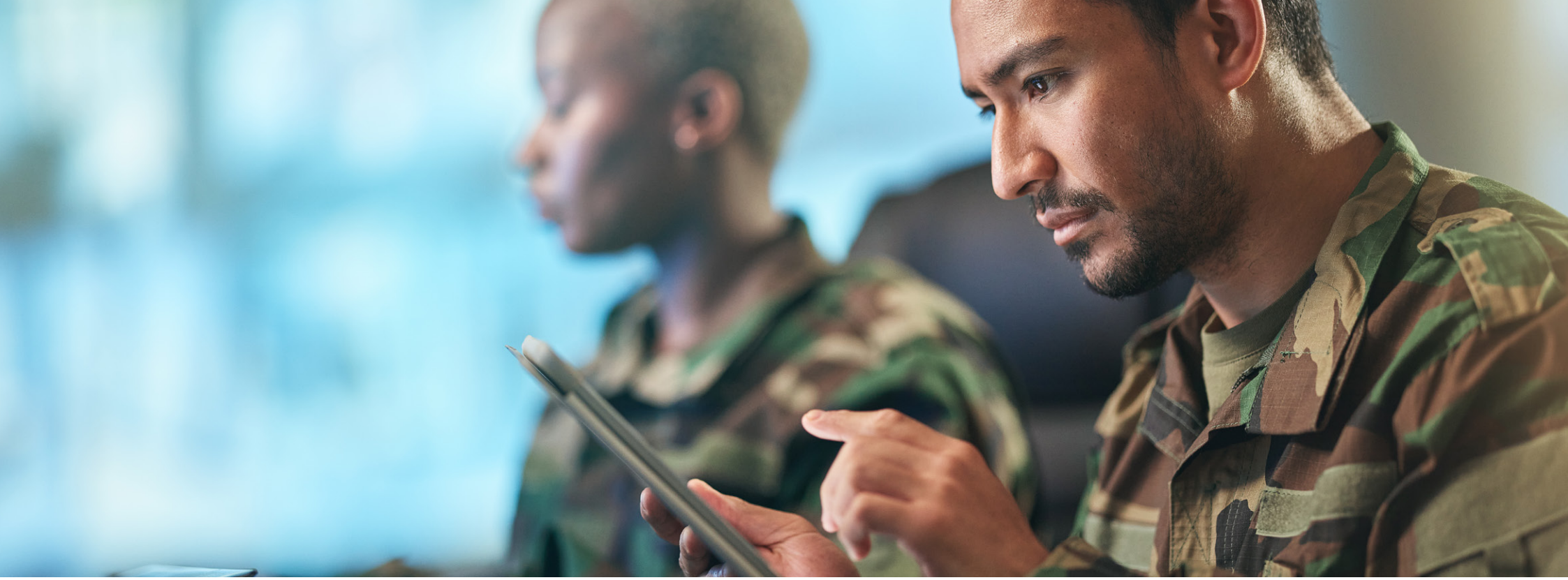
Aunque las estructuras heredadas –como la administración, los lugares de trabajo y las oficinas– pueden haber frenado una transformación en el pasado, las TIC han avanzado hasta el punto de que muchas de estas preocupaciones ya no son impedimentos para el progreso.

Con la estrategia de transformación digital y las tecnologías TIC adecuadas, las organizaciones de defensa ya pueden conectarlo todo, en todas partes. Esto les permitirá crear bases inteligentes, desde las que podrán cumplir más eficientemente los objetivos operativos en tiempos de paz y de conflicto, hacer frente más eficazmente a las ciberamenazas y atraer y retener más fácilmente a los mejores talentos.

Disponer de los datos adecuados en el momento oportuno puede reportar grandes beneficios: optimiza los procesos en el cuartel general y en las bases militares, facilita la toma de decisiones sobre el terreno con mayor conocimiento de causa y aumenta el personal y los equipos conectados en todas las zonas (tierra, aire, mar, espacio y ciberespacio).

En este documento, analizaremos los obstáculos a los que se enfrentan las organizaciones de defensa a la hora de emprender una transformación digital, así como los motores para hacerlo. Además, abordaremos los aprendizajes clave extraídos de organizaciones de los sectores público y privado que ya se han transformado y la manera en que pueden trasladarse al sector de la defensa.

1 - "Data Strategy for Defence: Delivering the Defence Data Framework and Exploiting the Power of Data", Ministerio de Defensa del Reino Unido, septiembre de 2021.



Obstáculos al cambio

Estructura interna

Uno de los mayores obstáculos a la transformación digital en el sector de la defensa es la propia naturaleza de las organizaciones de defensa. Los silos empresariales y tecnológicos han creado un entorno operativo único con sistemas de comunicaciones anticuados –como la telefonía basada en PBX– que no pueden soportar las modernas funciones de comunicación y colaboración.

En su mayor parte, los sistemas actuales funcionan en un entorno independiente, que no está conectado a Internet ni a ninguna infraestructura en la nube.

Así pues, mientras que gran parte del mundo comenzó su migración a la tecnología IP hace entre 10 y 20 años, el sector de la defensa se resistió por diversas razones:

- **Seguridad:** El cumplimiento de la normativa, los requisitos de privacidad y la necesidad de proteger los datos confidenciales dificultaban la adopción de cualquier tecnología que pudiera ser vulnerada
- **Cultura y gobernanza:** Una estructura de gestión vertical que exige la aprobación de los altos cargos para las principales iniciativas de cambio hizo que el ejército se perdiera la afluencia de la generación Y y de nativos digitales en los sectores público y privado. Esta nueva población creó una presión ascendente para adoptar las tecnologías digitales
- **Presupuesto:** Con recursos limitados, la prioridad ha sido mantener la disponibilidad de los equipos y el personal
- **Competencia:** A diferencia de las industrias comerciales, el sector de la defensa carece de competidores directos en la economía y se ha centrado principalmente en garantizar la destreza tecnológica de los activos del campo de batalla y los sistemas de guerra conectados

Impulsores del cambio

Geopolítica y tecnología

Al mismo tiempo que estos obstáculos han ido dificultando la transformación digital, el mundo ha experimentado un cambio espectacular.

La pandemia y la inestabilidad geopolítica han demostrado lo rápido que pueden interrumpirse las cadenas de suministro mundiales, con importantes efectos dominó en las economías locales.

Y el ritmo al que evoluciona la tecnología ha repercutido en los requisitos de gestión de datos.

Los avances en aprendizaje automático (AA), inteligencia artificial (IA), sensores avanzados y sistemas autónomos son la base de una generación de armas más sofisticadas y conectadas. Todas estas tecnologías están desempeñando un papel fundamental en los esfuerzos de defensa dentro y fuera del campo de batalla, y marcan el comienzo de un cambio hacia un proceso de gestión más centrado en los datos, tanto en casa como durante los conflictos.

Para optimizar los procesos y mantener un estado de preparación, toda organización de defensa debe encontrar formas eficientes y eficaces de recopilar, almacenar y distribuir todos los datos adicionales que generan estos nuevos sistemas.

Cooperación transversal

Para agravar la situación, se han introducido cambios más específicos en el marco en el que deben operar ahora las organizaciones de defensa.

Las delimitaciones tradicionales de las operaciones aéreas, terrestres y marítimas han dado paso a una visión global más compleja. Para ser eficaces, esos silos independientes deben formar parte ahora de un marco estratégico altamente conectado, centrado en operaciones multidominio y basado en la circulación fluida de datos dentro de todos los dominios y entre ellos.

La OTAN, por ejemplo, ha añadido el espacio y la cibernética a sus tradicionales operaciones marítimas, terrestres y aéreas como reconocimiento de la amenaza de los datos y la necesidad de orquestar mejor todos estos dominios.

Esto se complica aun más con los acuerdos de cooperación en materia de defensa que, según Brandon J. Kinne en su artículo Defense Cooperation Agreements and the Emergence of a Global Security Network, "establecen marcos institucionales a largo plazo para las relaciones bilaterales rutinarias de defensa, como la coordinación de políticas de defensa, ejercicios militares conjuntos, grupos de trabajo y comités, los intercambios en formación y educación, la investigación y desarrollo relacionados con la defensa y las adquisiciones".[2]

Estos acuerdos se basan en nuevos modelos operativos basados en el intercambio de información, el funcionamiento dinámico interconectado, la toma de decisiones ágil y rápida, la coordinación en tiempo real y la necesidad de resiliencia y seguridad de la información.

2 - "Defense Cooperation Agreements and the Emergence of a Global Security Network", Cambridge University Press, 2018.

"Dentro de la estructura de la OTAN existen cinco áreas de operaciones: marítima, terrestre, aérea, espacial y ciberespacial. Históricamente, las operaciones en estos ámbitos, o no han existido (es decir, el espacio y el ciberespacio), o han funcionado como entidades en gran medida independientes dentro de los ejércitos nacionales. Muchos ejércitos de naciones aliadas siguen funcionando hoy en día de este modo; sin embargo, dada la velocidad de la información, los flujos de datos y las capacidades del adversario, la necesidad de orquestar las actividades militares en todos los ámbitos como una fuerza única resulta crucial para las iniciativas de defensa y disuasión a largo plazo dentro de la OTAN."[3]

3 - "Multi-Domain Operations in NATO – Explained", OTAN, octubre de 2023.

Procesos de datos eficaces y seguros

En última instancia, para hacer posibles las operaciones multidominio y respaldar los acuerdos de cooperación en materia de defensa, todas las organizaciones de defensa necesitan sistemas que puedan mover datos de forma más eficiente y segura. Así pues, las organizaciones de defensa están adoptando rápidamente las normas IP y las tecnologías y sistemas de Internet de las cosas militares (IoMT) para hacer frente a la necesidad de recopilar y procesar cada vez más datos contextuales de buques, vehículos y activos no tripulados, y como dispositivos portátiles para soldados aumentados.

Pero aunque las tecnologías IoMT pueden recopilar datos, sigue siendo un reto proporcionar, distribuir y procesar de forma eficiente estos datos. En consecuencia, muchas organizaciones de defensa se plantean ahora la mejor manera de optimizar los procesos mediante la convergencia de los sistemas independientes de tecnología operativa (TO) y tecnología de la información (TI) en un marco operativo unificado.

Además, la evolución y sofisticación de la tecnología ha permitido a los países librar una ciberguerra más eficaz.

Por lo tanto, el alcance de los esfuerzos de protección en materia de defensa debe incluir ahora capacidades de disuasión digital contra ciberataques a infraestructuras críticas, así como campañas de desinformación, información errónea y mala información.

Obviamente, esto no puede hacerse con sistemas TIC anticuados y obsoletos. Y lo que es más importante, los sistemas anticuados y obsoletos no pueden soportar operaciones multidominio que incluyan el dominio cibernético. Tampoco pueden sustentar acuerdos de cooperación en materia de defensa con países socios que deben compartir información y tener la garantía de que esta estará protegida y segura.

Atracción y retención de empleados

El sector de la defensa se enfrenta a los mismos retos que las empresas comerciales: atraer y retener a los mejores talentos. Las organizaciones de defensa deben disponer de herramientas TIC para formar al personal en todos los ámbitos, crear un entorno de trabajo eficaz y gratificante y permitir el equilibrio entre vida laboral y personal que esperan ahora los empleados.

"...una empresa verdaderamente conectada ofrecerá integración, a escala nacional e internacional, en los cinco ámbitos: marítimo, terrestre, aéreo, cibernético y espacial. Esto permitirá a Defensa desatar plenamente el poder de sus datos, sensores de conexión y responsables de la toma de decisiones y ejecutores a escala y velocidad."[4]

MINISTERIO DE DEFENSA DEL REINO UNIDO

4 - "Data Strategy for Defence: Delivering the Defence Data Framework and Exploiting the Power of Data", Ministerio de Defensa del Reino Unido, septiembre de 2021.

Aprendizajes del sector público y privado

Aunque todos estos factores externos impulsan el cambio, muchas organizaciones de defensa siguen siendo lentas a la hora de adoptar estrategias de transformación digital, a pesar de que esta ha demostrado ser un medio eficaz para que las empresas públicas y privadas creen eficiencias y mejoren sus operaciones. Y como muchos de los trabajadores del sector de la defensa no son personal de combate, los planteamientos de la transformación y las lecciones aprendidas se aplican igualmente a los edificios de la administración de defensa y a las bases militares.

Las tecnologías TIC también han madurado hasta el punto de que muchas de las preocupaciones tecnológicas del pasado ya no son un problema. Existen soluciones digitales rentables y fáciles de implementar, basadas en protocolos estándar, que pueden prestar apoyo a los puestos de trabajo del sector de la defensa digital con comunicaciones y colaboración eficientes. Además, muchas proporcionan el alto nivel de defensa de ciberseguridad que necesitan las organizaciones.

La transformación digital estratégica equipará a las organizaciones de defensa para afrontar mejor la nueva realidad en la que operan. Una transformación eficaz creará un entorno digital seguro en el que todos los datos disponibles puedan moverse con mayor rapidez y seguridad para apoyar y capacitar al personal en todos los ámbitos. Y para crear ese entorno, las organizaciones de defensa pueden aplicar enfoques probados de transformación digital del sector privado y público.

En la siguiente sección, analizaremos lo aprendido implementando estrategias de transformación digital en los sectores público y privado y la manera de trasladar esto a las organizaciones de defensa.

Edificios inteligentes e infraestructuras hipeconscientes

Los edificios inteligentes han pasado a formar parte de los centros urbanos de todo el mundo y pueden crearse fácilmente en centros administrativos y bases militares del sector de la defensa. Estos edificios aprovechan las tecnologías IoT para supervisar y gestionar de forma inteligente todo, desde la iluminación y la calefacción hasta los sistemas de vigilancia en puntos clave de acceso y salida.

La continua evolución de las tecnologías IoT ha hecho posible la creación de infraestructuras hiperconscientes. Estas estructuras conectadas digitalmente combinan la automatización operativa con la gestión contextual del espacio para adaptar de forma inteligente el funcionamiento del edificio a las pautas de tráfico en zonas clave y a las necesidades de confort y seguridad de sus ocupantes y del entorno. El resultado son espacios inteligentes que hacen que los lugares de trabajo sean más seguros, saludables y felices, mejoran la experiencia de los empleados y aumentan la productividad.[5]

Conceptos de ciudad inteligente

Dado que las bases militares son similares a las ciudades autosuficientes, los edificios inteligentes y las infraestructuras hiperconscientes son ingredientes clave para crear bases inteligentes basadas en conceptos de ciudad inteligente de eficacia probada.

Las bases inteligentes aprovechan los datos disponibles en una base y crean "una infraestructura inteligente segura, edificios de bajo consumo, transporte eficiente, operaciones rentables y mayor calidad de vida para los habitantes".[6]

La infraestructura de red que permite una base inteligente también puede utilizarse para crear una posición de seguridad más eficaz que no solo proteja los datos de la base, sino también la seguridad física del personal y las instalaciones. Esto se puede conseguir con sistemas de seguridad avanzados, como la vigilancia perimetral y los sistemas de detección de intrusos creados con soluciones IoT e IA conectadas a los centros de seguridad.

Crear bases inteligentes va más allá de instalar los sensores y sistemas más novedosos. Se trata de integrar todas las tecnologías y procesos existentes y nuevos en un marco coherente de red TIC construido sobre las tecnologías más avanzadas y desplegado mediante una transformación digital estratégica.

Y esa transformación también puede aplicarse a otros ámbitos, como:

- Las operaciones sobre el terreno, donde las tecnologías TIC se utilizan como columna vertebral de las redes de información en buques y vehículos militares, y como enlace para un combatiente conectado que aprovecha sofisticados sensores y equipos portátiles
- Los centros de mando y control, donde las tecnologías TIC facilitan el apoyo a las operaciones de defensa civil o la gestión de crisis con otros organismos públicos durante catástrofes naturales

El poder de las TIC avanzadas

Con las tecnologías TIC más avanzadas, las organizaciones de defensa estarán mejor equipadas para compartir información, coordinar estrategias y gestionar operaciones conjuntas en cualquier lugar.

La clave para una transformación digital eficaz es un marco estratégico de comunicaciones y redes especialmente diseñado y optimizado para la base inteligente.

Esa red debe ser segura, sólida y estar diseñada para soportar todas las conexiones en todo momento, con el fin de mover con mayor eficacia enormes volúmenes de datos. Y debe construirse con soluciones TIC que apoyen la integración y la interconexión de las operaciones administrativas, las bases militares, el personal desplegado y los activos en tierra, aire, mar y espacio, así como la contención de las crecientes y perniciosas amenazas que se generan en el ciberespacio.

5 - "Smart Buildings Get Hyperaware", John Hatcher, Smart Buildings Magazine, agosto de 2020.
6 - "Building the Smart Base of the Future", Laura A. Nolan, National Strategic Research Institute, marzo de 2020.

ALE: Un socio para la transformación digital

Alcatel-Lucent Enterprise comprende los retos a los que se enfrentan las organizaciones de defensa a la hora de planificar y desarrollar estrategias de transformación digital que aprovechen las tecnologías TIC para satisfacer las demandas del ejército actual.

En ALE, apoyamos la transformación digital con soluciones resistentes y seguras para la defensa conectada, incluyendo:

- Soluciones LAN y WLAN habilitadas para IoT, incluyendo conmutadores robustos que satisfagan los requisitos de la red y proporcionen una incorporación segura y automatizada del IoT para una variedad de requisitos de la defensa conectada
- Soluciones de comunicaciones, colaboración y CPaaS que pueden ofrecerse en las instalaciones (nube privada), en la nube pública o en un modelo híbrido
- Soluciones de automatización de flujos de trabajo y procesos que supervisan y detectan y abordan proactivamente determinadas cuestiones antes de que se conviertan en problemas, aumentando así la eficiencia operativa y reduciendo los costes
- Seguridad con la privacidad por diseño construida en un marco de confianza cero y con todas las certificaciones de privacidad de datos pertinentes en los países en los que operamos

Las soluciones de comunicaciones y redes de ALE pueden optimizarse para crear arquitecturas redundantes que conecten a todos y a todo en un marco cohesivo, totalmente integrado y de alta disponibilidad.

Además, nuestras soluciones están diseñadas pensando en la máxima seguridad. Cumplimos estrictamente las prácticas y normas de seguridad actuales e incorporamos a nuestros productos una serie de tecnologías relacionadas sin coste adicional. La seguridad se basa en un enfoque por capas que incluye la integridad de la red, la seguridad de los dispositivos y las políticas de acceso basadas en los perfiles de usuario y la visibilidad de las aplicaciones. El software de red se verifica mediante la validación por terceros del código subyacente. Los sistemas y usuarios del IoT se incorporan de forma automática y segura y se colocan en contenedores, que están estructurados para evitar posibles ciberataques desde un dispositivo comprometido. Y todos los datos y comunicaciones se cifran con fuertes mecanismos de cifrado para evitar el espionaje y los ataques de intermediarios.

Para mayor tranquilidad, nuestras soluciones también cumplen los certificados de seguridad más exigentes emitidos por organizaciones independientes e instituciones gubernamentales.

Además, nuestro marco de riesgo, resiliencia y seguridad (RRS) aborda la seguridad cibernética y física para los sectores gubernamental y de defensa.

También comprendemos la importancia de la soberanía de los datos. Nuestras aplicaciones basadas en la nube ofrecen opciones de alojamiento flexibles: en centros de datos avanzados y altamente seguros construidos para proporcionar un rendimiento rápido y fiable, o en las instalaciones con nuestra solución de nube privada Rainbow Edge. Los datos almacenados en la nube son propiedad de nuestros clientes. Nosotros no proporcionamos ni vendemos datos a ninguna otra empresa o país.

Más información

Para obtener más información sobre las soluciones de Alcatel-Lucent Enterprise para la industria de defensa, visite nuestro sitio web o póngase en contacto con nosotros para hablar sobre cómo podemos ayudarlo a desarrollar una estrategia de transformación digital personalizada para su organización de defensa.

Alcatel·Lucent
Enterprise