Modernización digital: desafíos de los sistemas de información y comunicaciones para lograr la superioridad de la información en el entorno táctico

Autores: Isabel Iglesias Pallín, Bernardo Martínez Reif, OT TICS. SDG PLATIN

Palabras clave: digitalización, sistemas heredados, comunicaciones tácticas y sistemas de información, mando y control, superioridad de la información.

Metas Tecnológicas relacionadas: MT 6.1.1., MT 6.1.2., MT 6.1.3., MT 6.2.4., MT 6.4.2., MT 6.5.1.

Resumen

La transformación digital de las Fuerzas Armadas requiere la creación de un proceso estructurado y escalable para garantizar la preparación de la misión. Las implementaciones de sistemas modernos coexisten con los sistemas heredados. Una plétora de plataformas, nodos y fuentes de información integran un campo de batalla hiperconectado. Este artículo analiza los desafíos en la búsqueda de soluciones armonizadas en el campo de las comunicaciones y los sistemas de información y especialmente en el entorno táctico, que es uno de los ámbitos más exigentes a la hora de garantizar la disponibilidad e interoperabilidad. Las tecnologías emergentes como la Inteligencia Artificial, Internet de las Cosas y otras relacionadas con la automatización están en el centro de esta transformación.

Introducción

La transformación digital es un hecho en nuestra sociedad. Los servicios digitales están impregnando cada área de nuestras vidas. Casi sin darnos cuenta, sectores como la comunicación, las finanzas, la fabricación, el comercio o el entretenimiento se

Fig. 1. Digitalización (Fuente: Pixabay)

están volviendo más digitales y más conectados. Hace unos años, sintonizábamos la radio en lugar de instalar una aplicación para escuchar nuestras canciones favoritas almacenadas en nuestra propia lista de preferencias. No es necesario alquilar la última película en el video club más cercano un año después de su estreno en el cine y devolver la cinta de video 24 horas después. Ahora disponemos de numerosas plataformas de medios en nuestra propia sala de estar y podemos ver el último estreno pulsando un botón del mando a distancia de nuestra televisión. Existen multitud de ejemplos de cómo se hacían las cosas antes y cómo se hacen ahora, por ejemplo: mensajería instantánea, transporte compartido o redes sociales.

La sociedad demanda servicios que requieren ubicuidad, simplicidad, eficiencia, confiabilidad, seguridad y velocidad. Estas características exigen tecnologías digitales que brinden accesibilidad rápida, conectividad generalizada, automatización y resistencia.

La transformación digital ha cambiado las "reglas del enfrentamiento" de nuestro día a día en áreas como las relaciones sociales, el consumo, el trabajo, etc.… Defensa no puede quedarse atrás en este proceso imparable: nuestros combatientes en operaciones, ya sean marítimas, terrestres o aéreas, esperan utilizar ventajas digitales similares a las del mundo civil. Las especiales características del contexto del trabajo que realizan las Fuerzas Armadas plantean desafíos y cuestiones adicionales para construir un ecosistema digital adaptado a las misiones: la información debe preservar su confidencialidad, integridad y disponibilidad bajo cualquier circunstancia, se requiere de equipos especiales para resistir las condiciones adversas de las inclemencias del tiempo, o se requiere conectividad permanente en lugares donde no existe una infraestructura de telecomunicaciones permanente. Esto lleva a los militares a ser más precisos y rigurosos al definir requisitos específicos y verificar su cumplimiento antes de lanzar productos o soluciones. Se debe definir un conjunto de necesidades en términos de requisitos mediante el análisis de distintos escenarios. La ingeniería de sistemas asegurará un enfoque metodológico para identificar y validar estos requisitos de usuario.

En el campo de batalla, un combatiente debe tener una consciencia clara de la situación que incluya una evaluación de las amenazas, la ubicación de las fuerzas enemigas, los detalles de la orografía del terreno, la infraestructura disponible, los puntos de suministro, etc.

La información sobre la misión es clave para el cumplimiento de sus ta-

reas. Los flujos de información siguen una ruta múltiple de transmisiones y recepciones de órdenes entre unidades tácticas y escalones de mando superiores respaldados por una red de comunicaciones de gran alcance.

La información proporcionada al combatiente tiene que ser útil para tomar decisiones en pocos segundos. La mayoría de las veces no hay posibilidad de analizar la información disponible. Esto podría conducir a una situación de sobrecarga de información. Se deben llevar a cabo actividades de investigación que desarrollen nuevas interfaces entre el humano y el sistema y que presente esta información a los usuarios finales como un conocimiento útil que les permita elegir una opción entre varias alternativas, pero sin saturarle.

Por otra parte, garantizar la libertad de acceso al ciberespacio es primordial. Una de las tareas principales de este ámbito es proteger los sistemas y las redes, incluidos los datos de misión crítica, contra los ataques cibernéticos.

El campo de batalla se está viendo transformado gracias a un sinfín de tecnologías disruptivas que han llegado para quedarse. Tecnologías como *Big Data* para facilitar un análisis rápido de grandes cantidades de datos, Internet de las cosas y sensores utilizados como fuentes de información e Inteligencia Artificial para ayudar a la toma de decisiones, son habilitadores a nivel táctico y hay multitud de aplicaciones que pueden darse a estas tecnologías en el futuro y que aún tienen que ser probadas.

Consecuencias del rápido ritmo del desarrollo tecnológico

Las consecuencias inmediatas de esta vertiginosa exigencia tecnológica se pueden resumir en una interconectividad de la red sin precedentes, la necesidad de información en tiempo real para alimentar los ciclos de decisión y la abundancia de datos sin procesar. Las demandas de procesamiento de datos han cambiado en términos del volumen de datos a procesar y la velocidad de este procesamiento de datos.

Nuestra sociedad digital es predominantemente una sociedad de *Big Data* caracterizada por las conocidas 5 Vs

Fig. 2. Transformación digital (Fuente: Pixabay)

que definen un tipo muy concreto de problemas a resolver: Volumen, Velocidad, Variabilidad, Veracidad y Valor. Es decir, además de las ya mencionadas, otras características como la heterogeneidad de los tipos de datos a procesar (video, imágenes, audio, señales de dispositivos, entre otros), la veracidad de la información a tratar y la necesidad de que todo este esfuerzo produzca resultados con valor, marcan las expectativas del usuario con respecto a estas tecnologías. Todo ello lleva a requerir la información exacta y precisa en el momento adecuado utilizando una aplicación adecuada que ayude a tomar la mejor decisión posible en función de la información contextual disponible.

En el campo de batalla, el ejército necesita además lograr una clara consciencia situacional. Una imagen operativa común ayuda a interpretar en un Sistema de Información Geográfica diferentes capas de información (instalaciones, clima, puentes, fuerzas, etc.) y amenazas (posiciones enemigas, terreno, cobertura de señales, clima, entre otros).

Para poder soportar los servicios antes mencionados, las configuraciones de los sistemas y redes deben ser flexibles, adaptándose incluso a las peores condiciones que puedan presentarse y, si fuera necesario, autoconfigurarse de acuerdo con las necesidades de la misión. Tecnologías como la red definida por software (SDN) y la virtualización de funciones de red relacionadas (NFV) permiten obtener mayor rendimiento de los recursos de la red. Algunas de las principales dificultades en la implementación de SDN en redes tácticas residen en la alta movilidad de los nodos finales, un ancho de banda limitado junto con enlaces inalámbricos de baja velocidad de datos, la adopción de medidas de seguridad cibernética y la importancia de garantizar la interoperabilidad.

CIS táctico a la vanguardia de la transformación digital

Los Sistemas de Información y Comunicaciones Tácticas (CIS) abordan las telecomunicaciones y los servicios militares que permiten a pequeñas unidades, equipos o combatientes individuales cumplir una misión. Podrían verse como la "última frontera" en una estructura jerárquica de telecomunicaciones que a menudo se conoce como *tactical edge*.

El entorno táctico es un laboratorio de experimentación donde no se permiten fallos. La flexibilidad y la adaptabilidad son dos características a conseguir para aprovechar los recursos disponibles en cada momento. Se pueden encontrar un buen número de aplicaciones de tecnologías emergentes que sirven de ejemplo como escenarios para este laboratorio: la ciberseguridad, las tecnologías cuánticas, la Inteligencia artificial, los drones o el procesamiento en la nube son algunas de ellas.

Fig. 3. Comunicaciones en ET. (Fuente: Ejército de Tierra)

Además, es necesario agregar y sintetizar la información de la manera más adecuada para presentarla en los niveles superiores: el operativo y el de mando estratégico. La interoperabilidad entre los diferentes dominios de la guerra, los físicos, terrestre, aéreo y marítimo, pero también el espacio y el ciberespacio, es un factor determinante. La información debe fluir entre dominios y cada nuevo bit de información debe ser complementario a la información disponible. La interoperabilidad se vuelve más importante aún si cabe para las fuerzas de coalición donde cada sistema ha sido desarrollado por equipos distintos con una conceptualización y unos requisitos diferentes. La importancia de la semántica y el desarrollo de ontologías, permite que sistemas de coalición de diferente naturaleza, puedan entenderse y cooperar en el campo de batalla.

El entorno CIS táctico y los problemas de seguridad en el ámbito digital plantean muchos desafíos por superar. Por un lado, el CIS debe poder operar de manera segura en un entorno digital de rápido desarrollo y garantizar la preparación de la misión. Por otro lado, deben garantizar permanentemente la libertad de acceso al ciberespacio, que no es solo un dominio transversal, sino también un dominio en sí mismo en el que las amenazas cibernéticas que afectan a la misión son numerosas, p.ej. la disrupción de infraestructuras críticas. En un mundo que despliega cada día más servicios digitales, las ciberamenazas evolucionan cada vez más. En ocasiones hasta más rápido que los propios servicios.

Por lo tanto, habrá que poner el foco en la protección cibernética de los activos, así como las capacidades para mejorar la detección de ataques cibernéticos. La seguridad debe estar en la mente de los ingenieros desde el diseño de los componentes digitales y debe seguirle una ingeniería de seguridad proactiva que provea unos sistemas de información y comunicaciones ciberresilientes. La ciberdefensa es aún más necesaria no solo para proteger los sistemas, sino también para anticipar o prevenir la ocurrencia de ciberataques. La inteligencia sobre amenazas cibernéticas es una disciplina emergente que analiza los vectores de ataque utilizados para explotar vulnerabilidades y propone medidas de mitigación de riesgos.

Todos los activos militares deberán incluir capacidades para resistir nuevas formas de ciberataques con la llegada de la computación cuántica y las tecnologías de comunicación cuántica. En entornos de coaliciones multinacionales, la confianza digital es probablemente el aspecto más difícil cuando los usuarios se unen, agrupan o abandonan una infraestructura de red de forma dinámica.

Con el paradigma de todo conectado en el campo de batalla, una definición de nodos finales en este contexto se aplicaría necesariamente por igual a plataformas y sensores. La proliferación de vehículos aéreos, terrestres y submarinos (UXV) no tripulados, habilitados por algoritmos de IA, pone un mayor énfasis en la formación de equipos entre humanos y máquinas. La colaboración con estos robots operando como un enjambre alcanza otro nivel superior de complejidad en la gestión de la infraestructura de comunicaciones digitales. El establecimiento de prioridades, la calidad del servicio y las características de segmentación dinámica de la red podrían mejorar las propiedades de una red potencialmente saturada que soporte un “sistema de sistemas”.

Hablando de redes desplegables y, en particular en el borde táctico, existe una tendencia creciente a explorar aplicaciones novedosas de una “*nube de combate*” para aliviar las limitaciones de ancho de banda de la red y potencia de procesamiento. Una red táctica conectada a la nube puede aportar nuevos avances al acelerar los intercambios de información.

La superioridad de la información como objetivo final

Hoy en día, nuestro mundo se ha vuelto cada vez más digital y virtual. En los próximos años, se espera que esta tendencia se acelere y tenga efecto en las operaciones y capacidades militares. Los conjuntos de datos están aumentando con una magnitud difícil de manejar. Los sensores distribuidos, la autonomía, las nuevas tecnologías de la comunicación y el desarrollo de nuevos métodos analíticos aumentarán la capacidad de comprender la información que nos rodea.

Los conflictos actuales se caracterizan por una complejidad cada vez mayor que exige el manejo de enormes y heterogéneos volúmenes de información y, simultáneamente, solicita tiempos de reacción más cortos. Para hacer frente a escenarios bélicos híbridos, será necesario no solo centrarse en las áreas de guerra clásica y emergente, sino también analizar otros dominios sociales para lograr adecuadamente la conciencia situacional requerida.

Esto requerirá fortalecer las capacidades relacionadas con la recopilación de datos y su rápida transfor-

mación en información valiosa para apoyar las decisiones de los comandantes y coordinar adecuadamente múltiples fuerzas en múltiples niveles en operaciones conjuntas. La superioridad de la información jugará un papel aún más crucial para que las Fuerzas Armadas protejan a sus ciudadanos de amenazas externas y enfrenten de manera eficiente crisis futuras.

Estrechamente relacionada con este requisito está la necesidad de contar con un CIS táctico con un mayor grado de interoperabilidad. La complejidad de los conflictos futuros y la variedad de fuerzas que participan en las operaciones requieren de la capacidad de interactuar en diferentes niveles, que van desde la comunicación física hasta el intercambio automático de datos de un sistema a otro. Para garantizar esto, es necesaria una sólida gestión, protección y explotación del espectro electromagnético y del ciberdominio. No se puede lograr la superioridad de la información si ésta y los datos que la originan no se manejan adecuadamente. La proliferación de sensores militares, desde satélites hasta micro-drones, generará grandes cantidades de datos que deben transmitirse, compartirse y procesarse de manera efectiva. Las capacidades de gestión de la información deben mejorarse para apoyar a los comandantes que tienen que lidiar con grandes cantidades de información proveniente de múltiples y heterogéneas fuentes de información.

Un nivel superior en esta interoperabilidad es la interoperabilidad semántica, que además de dar especial importancia al significado de los conceptos pactados en una ontología militar, cuenta con mecanismos para clasificar información o inferir conocimientos.

El *Big Data* será crucial para mejorar las capacidades militares. La inteligencia artificial, en particular, requiere datos de entrenamiento de alta calidad para desarrollar nuevos algoritmos y aplicaciones.

Estas tecnologías aumentarán la eficiencia operativa, reducirán los costes, mejorarán el conocimiento de la situación en los niveles estratégico, operativo y táctico y tienen el potencial de crear una ventaja en la toma de decisiones.

El uso de inteligencia artificial en sensores para preprocesar información y proporcionar un uso adaptativo de frecuencias y ancho de banda tendrá un impacto en las comunicaciones militares. Los sensores proporcionan datos en el dominio físico. El concepto de sensores desplegados, la capacidad de detectar y rastrear cualquier objeto a distancia procesando los datos adquiridos por ellos, se verá habilitado significativamente por el crecimiento de la comunicación 5G y el Internet de las cosas (IoT). Todo será un sensor y todos los sensores estarán conectados en red. Las aplicaciones militares serán de amplio alcance, incluido el desarrollo de una *Common Operational Picture* multidominio.

El análisis y las técnicas computacionales avanzadas para el procesamiento y la fusión de datos mejorarán los rangos de los sensores y brindarán información contextual más rica. La inteligencia artificial, específicamente el aprendizaje automático, es una técnica computacional prometedora capaz de procesar grandes volúmenes de información. Estas herramientas predictivas son valiosas para detectar intenciones y predecir posibles acciones y eventos futuros. Mientras tanto, la computación cognitiva puede verse como una integración de algoritmos y métodos de diversos campos como la inteligencia artificial (IA), el aprendizaje automático, el procesamiento del lenguaje natural (PNL) y la representación del conocimiento para mejorar el desempeño humano en tareas cognitivas. Los futuros sistemas serán capaces de aprender y comprender el lenguaje natural, así como la razón, e incluso interactuar de forma más natural con los humanos que los sistemas programables tradicionales. Los sistemas de computación cognitiva pueden complementar el trabajo humano en tres capacidades: mayor participación, mejor toma de decisiones basada en evidencia y descubrimiento de conocimientos ocultos en grandes cantidades de datos.

La comunicación segura y el almacenamiento de datos son esenciales en las operaciones militares. Las bases de datos son los medios tradicionales para almacenar y mantener datos estructurados y relacionados. Las tecnologías de control distribuido, como *blockchain*, han surgido y se han utilizado como gestión de datos distribuida y permanente. El mayor uso de tecnologías *blockchain* incrementará la capacidad militar para garantizar comunicaciones confiables y almacenamiento de datos.

El papel de la ingeniería de sistemas y el desarrollo arquitectónico

La ingeniería de sistemas es otro aspecto en el que la transformación digital debe jugar un papel importante. Los ciclos de vida tradicionales, como las redes y los sistemas heredados, ya no pueden proporcionar las mismas respuestas a los ingenieros y desarrolladores de la nueva era digital. Las necesidades evolucionan cada vez más rápidamente. Por tanto, el uso de metodologías ágiles es más que conveniente para afrontar estos cambios

Fig. 4. Aplicaciones en la palma de la mano. (Fuente: Pixabay)

y poder cumplir con las restricciones de los sistemas en un corto período de tiempo. Estas metodologías, como *Scrum*, se caracterizan por presentar frecuentemente prototipos al usuario final, pruebas de concepto y diseños modulares que avanzan en paralelo con el desarrollo del producto. Todo ello, teniendo en cuenta todas las posibilidades o escenarios futuros de uso para convertirlos en modelos adaptables.

La innovación también debe estar presente con arquitecturas adaptativas que combinen diferentes modelos de aprendizaje (por ejemplo, aprendizaje supervisado y no supervisado), según sea necesario en el momento, nubes privadas e híbridas y *Edge computing* donde el procesado de los datos se realiza dondequiera que la información sea recopilada por dispositivos o sensores para minimizar los tiempos de latencia en la transmisión.

Asimismo, en el mundo de la representación del conocimiento, las bases de datos relacionales también están dando paso a bases de datos no relacionales, esquemas XML y ontologías que inciden en la semántica de los conceptos que se manejan.

Tecnologías para la hiperconectividad

Las batallas se libran principalmente en lugares desiertos, donde las comunicaciones no son óptimas e imponen dificultades en términos de potencia, latencia o fluctuación del retardo debido a ruido indeseado (*jitter*). Esto se debe a dos cosas, primero, que las condiciones ambientales no son adecuadas, y segundo, que los dispositivos no están preparados para soportar estas condiciones límites. Por tanto, es necesario mejorar la interconectividad de los sistemas y brindar una mejor comunicación que permita a los soldados moverse por el campo de batalla, permaneciendo continuamente interconectados.

En primer lugar, es posible hacer uso de las comunicaciones por satélite de nueva generación. También se utilizan redes tácticas desplegadas, que son un conjunto de entidades militares interconectadas, a través de las cuales los soldados pueden comunicarse en las campañas o durante el transcurso de la misión, con el fin de mejorar la consciencia situacional.

El uso de estas redes plantea algunos desafíos en términos de ciberseguridad en entornos de peligro: ancho de banda limitado, poco almacenamiento de datos y enlaces inalámbricos poco fiables o de baja velocidad de datos, que pueden abordarse mediante el uso de redes cognitivas y redes definidas por software (SDN) entre otras.

Ambas tecnologías se complementan y fomentan el uso conjunto. La primera de ellas, permite realizar una optimización del espectro y encontrar bandas de frecuencia libres sobre las que transmitir información. Desde un punto de vista operativo, puede asegurar una comunicación ininterrumpida con soldados aliados o con sistemas de apoyo, sin necesidad de que estos sean fijos. Sus principales características son:

- **Flexibilidad:** un único sistema que aprovecha la infraestructura existente y permite conexiones por cable o inalámbricas. También es compatible con múltiples frecuencias.
- **Alto rendimiento**: altas velocidades de transmisión en el nivel IP y gran alcance de enlace.
- **Facilidad de integración**: admite la integración de radios de combate y diferentes tipos de protocolos de comunicación.
- **Facilidad de gestión**: configuración sencilla con una red autoorganizada y una interfaz intuitiva.

Sin embargo, por otro lado, también tiene algunos inconvenientes que deben abordarse:

- Necesitan interconectividad a través de diferentes capas de la red.
- Es necesario mejorar la comunicación para aumentar el rango de movilidad de los combatientes.
- El desarrollo e implementación de estos sistemas tiene un alto coste.

Algunos de estos inconvenientes se pueden abordar mediante el uso del segundo tipo de redes previamente comentado (SDN), que se basa en la separación del plano de control y el plano de datos o aplicación. Esta técnica ofrece mayor flexibilidad, agilidad y eficiencia, además de reducir el *hardware* necesario. Con ello se reducen los costos operativos y de material.

Por tanto, el uso de estas tecnologías, permite mejorar la movilidad de los combatientes, aprovechar la infraestructura ya existente por la Redes de Misiones Federadas (FMN) de la OTAN y evitar la existencia de un único punto de fallo. Si bien, debido al estado de desarrollo en el que se encuentran, no están completamente operativos, por lo que los soldados deben poder ejecutar misiones de manera independiente, hasta que se desplieguen modelos robustos y confiables de estas redes.

Conclusiones

La transformación digital es un hecho que los sistemas, redes y comunicaciones tácticas no pueden ignorar. Debemos acompañar este progreso y beneficiarnos de él para brindar a nuestras Fuerzas Armadas los mejores medios en el teatro de operaciones para llevar a cabo su misión.

La cooperación es fundamental para acelerar el ritmo de adaptación. Reutilizar el trabajo realizado por otros y avanzar desde ese punto hacia adelante debe ser una máxima para, finalmente, compartir los resultados con toda la comunidad interesada en estos avances. Hay que perder gradualmente la noción de propiedad individual para adquirir la noción de propiedad colectiva.

Para que esto suceda, es necesario avanzar con pasos seguros y firmes. La transición a nuevas tecnologías debe suavizarse, permitiendo que las soluciones heredadas coexistan con los nuevos desarrollos. El cambio debe ser progresivo y la tecnología debe adaptarse a las necesidades.

Para acompañar este avance, el CIS táctico contará con algunas tecnologías habilitadoras, como la Inteligencia Artificial, la hiperconectividad, el Internet de las Cosas (IoT), la computación en el borde (*Edge Computing*) y la ciberinteligencia entre otras. El uso y aplicación de estas tecnologías proporciona al nivel táctico CIS una mayor consciencia situacional y una superioridad de la información que el combatiente no solo ya necesita, sino que está siendo exigida.

Referencias

[1] Fiott, Daniel. Digitalising Defence, Protecting Europe in the age of quantum computing and the cloud, Brief 4, Institute of Security Studies, March 2020.

[2] Modular and adaptive tactical network to control, change and manage network behaviour, including cyber security consulted at

[3] https://eda.europa.eu/webzine/issue16/cover-story/cyber-resilience-a-prerequisite-for-autonomous-systems-and-vice-versa/

[4] Jesús Gómez Ruedas. Instituto Español de Estudios Estratégicos (ieee.es). Documento marco "Despega la transformación digital del Ministerio de Defensa" November 2015

[5] Industria 4.0 en los sectores aeroespacial y de Defensa

[6] Dr. José Luis Jiménez Martín. Dpto. de Ingeniería Audiovisual y Comunicaciones. EUITT. Universidad Politécnica de Madrid. "Tecnologías aplicadas al Mando y Control. Sistemas C4ISR" October 2010

[7] Instituto Español de Estudios Estratégicos (ieee.es). Cuadernos de Estrategia 179 "Análisis comparativo de las capacidades militares españolas con las de los países de su entorno" August 2016

[8] Ejército de Tierra. Resumen ejecutivo 'FUERZA 35'. 2019.

[9] Ejército de Tierra. Fuerza 35. 2019

[10] Revista de Aeronáutica y Astronáutica 890. Dossier (pags 66-94). February 2020

[11] Revista general de la Marina. Apoyo logístico 4.0. September 2018.

[12] Raúl Arrabales. ICEMD, El Instituto de la Economía Digital. "Computación Cognitiva. La nueva revolución del Big Data". January 2016.

[13] https://www.janes.com/defence-news/news-detail/darpa-sees-rich-space-for-advanced-ai-in-cyber-operations

[14] Gansler J. S., Lucyshyn W., Rigilano J., The Joint Tactical Radio System: Lessons Learned and the Way Forward, Center for Public Policy and Private Enterprise, February 2012

[15] Marrone A., Nones M., Ungaro A. R., Technological Inovation and Defence: The Forza NEC Program in the Euro-Atlantic Framework, Instituto Affari Internazionali, 2016

[16] Rose L., Massin R., Vijayandran L., Debbah M., Martret C. J., CORASMA Program on Cognitive Radio for Tactical Networks: High Fidelity Simulator and First Results on Dynamic Frequency Allocation, European Defence Agency, 2013

[17] Dura M., RADMOR ready to design the 'European' Programmable Radio, Defence 24, 16th December 2015