eDossier

TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES

Tendencias actuales en los desarrollos TIC destinados a las Fuerzas Armadas y soluciones propuestas por la industria española

Carlos Calvo González-Regueral y Roberto Obeso Cobo

Diciembre 2022

Informe patrocinado por

aesmide
Asociación de Empresas Contratistas con las Administraciones Públicas

GOBIERNO DE ESPAÑA
MINISTERIO DE INDUSTRIA, COMERCIO Y TURISMO
ICEX
UNIÓN EUROPEA

ids

Carlos Calvo González-Regueral es coronel (reserva) del Ejército de Tierra. Durante su tiempo en servicio activo estuvo destinado en diferentes unidades operativas y logísticas y en Estados Mayores (nacionales e internacionales). Ha estado destinado en la Dirección General de Armamento y Material del Ministerio de Defensa donde, como coronel, fue jefe del área de planificación. Es veterano de operaciones en Bosnia Herzegovina y Kosovo. Ha realizado diferentes cursos sobre adquisiciones de sistemas de armas en España, Alemania, Francia y la Agencia Europea de Defensa. Es autor de más de 100 artículos y es colaborador habitual de IDS.

Roberto Obeso Cobo es licenciado en Físicas, Ingeniero de Materiales y máster en Ingeniería de Organización y Logística. Actualmente trabaja como ingeniero de sistemas en la empresa Isdefe, donde presta asistencia técnica a la Dirección General de Armamento y Material del Ministerio de Defensa en el proceso de planeamiento y programación de recursos de armamento y material. También es profesor asociado en la Universidad Carlos III de Madrid, donde imparte docencia en el máster de Ingeniería Industrial y en el grado de Tecnologías Industriales. Ha realizado numerosos cursos en materias TIC y ha colaborado en el desarrollo de temarios universitarios como el de Tecnologías de la Información y las Comunicaciones para la Logística.

Contenidos

Prólogo

Teniente General José María Millán Martínez
Director del Centro de Sistemas y Tecnologías de la Información y las Comunicaciones (CESTIC)

La transformación digital, el dato como activo estratégico, el 5G, la inteligencia artificial, la computación cuántica, la nube de combate, el ciberespacio, son conceptos que se han añadido de forma brusca al acervo del idioma corriente. Por eso es de agradecer la iniciativa de Aesmide e IDS. Este ejemplar de la serie de publicaciones digitales permite acceder de una manera coherente a las soluciones que ofrecen sus asociados, relacionándolas con las necesidades militares, claramente expuestas en este caso, por Carlos Calvo y Roberto Obeso.

El hombre se ha acostumbrado tanto a la tecnología que no aprecia la enorme complejidad técnica de los conceptos recogidos en este dossier. Sostenemos en la mano un terminal móvil con el que podemos (literalmente) acceder con perfección e inmediatez al saber universal, sin siquiera reflexionar una milésima de segundo en lo que hay detrás de una simple búsqueda en internet: una ingente masa de tecnología, de ingeniería, plataformas de información (centros de datos, motores de búsqueda, algoritmos, inteligencia artificial), redes de comunicaciones (altas torres de radioenlaces o interminables tendidos de fibra óptica, urbanos, rurales, intercontinentales), sistemas de seguridad, bases de datos, equipos de soporte, de monitorización, de atención al usuario.

El combatiente, hombre de su tiempo, necesita en la trinchera esta misma respuesta tecnológica inmediata y universal, sin reparar en que es preciso desplegar en el teatro de operaciones una infraestructura similar a la que he descrito. Para él es invisible. He aquí la dificultad del combate actual: desenvolverse en la esfera digital en la que estamos inmersos, y vencer en este combate.

Para evitar el vértigo que produce lo perfecto, es recomendable la lectura de este dossier: encierra varios esfuerzos. Uno de síntesis: se centra en lo más relevante; otro divulgativo: acude a las soluciones que las empresas nacionales ofrecen a los problemas que se plantean. Y el más importante, y como los anteriores, exitoso: la lectura es amena.

Nos felicitamos de la iniciativa y saludamos su materialización, y esperamos que sea una herramienta útil para mostrar las capacidades de nuestra industria, es decir, de nuestra nación.

1. Consideraciones generales

Si algún ámbito de actividad o avance tecnológico responde al paradigma del impulso de las actividades civiles sobre los ámbitos de defensa y seguridad, este es precisamente el de las tecnologías de información y comunicaciones.

Se trata de un amplio conjunto de tecnologías que nos alcanzan en todas nuestras actividades cotidianas y que tienen un impacto transversal en distintos campos. En el ámbito específico militar, la necesidad de disponer de una capacidad de mando y control para poder, planear, conducir y realizar operaciones es la base del empleo del resto de capacidades, tanto a nivel estratégico, como en los campos operacional y táctico.

Se trata de un amplio conjunto de tecnologías que alcanzan todas nuestras actividades cotidianas

En el presente documento repasaremos de forma somera cual es la situación actual y las tendencias en cuanto a las necesidades que se presentan, así como las principales áreas de tecnologías relacionadas con servicios de información y comunicaciones. Repasaremos, también de forma somera, las principales iniciativas que se están abordando a nivel europeo para mejorar las capacidades de cara a obtener una mayor autonomía estratégica en unas tecnologías que son críticas, así como, la visión que ofrece el Ministerio de Defensa español.

Presentamos también cual es el panorama de oferta de servicios, desde la perspectiva de las empresas asociadas en Aesmide, que permite ofrecer una amplia panoplia de capacidades para satisfacer las necesidades de los clientes.

2. Situación actual

Las tecnologías de la información y las comunicaciones (TIC) llevan años impregnado todas las capas de la sociedad y han supuesto una revolución a todos los niveles: la manera trabajar, de comunicarnos e incluso de relacionarnos han cambiado con cada nuevo desarrollo o nueva tecnología. Adoptar estas tecnologías de manera masiva ha traído muchas ventajas y comodidades, pero, como contrapartida, ha generado una altísima dependencia y muchos riesgos. Las consecuencias cuando fallan estos sistemas son muy graves y pueden llegar a paralizar sectores de la economía.

La adopción de las TIC, lejos de integrarse de una manera suave o lineal, se produce de manera cada vez más rápida. La famosa ley de Moore, que predice un aumento exponencial de la capacidad de cómputo de los ordenadores, nos da una idea de la velocidad de desarrollo de estas tecnologías.

Este nuevo paradigma de empleo de tecnologías TIC ha configurado, a nivel industrial, lo que se conoce como Cuarta Revolución Industrial o Industria 4.0, utilizando una terminología heredada del sector de la informática. Sin embargo, estas

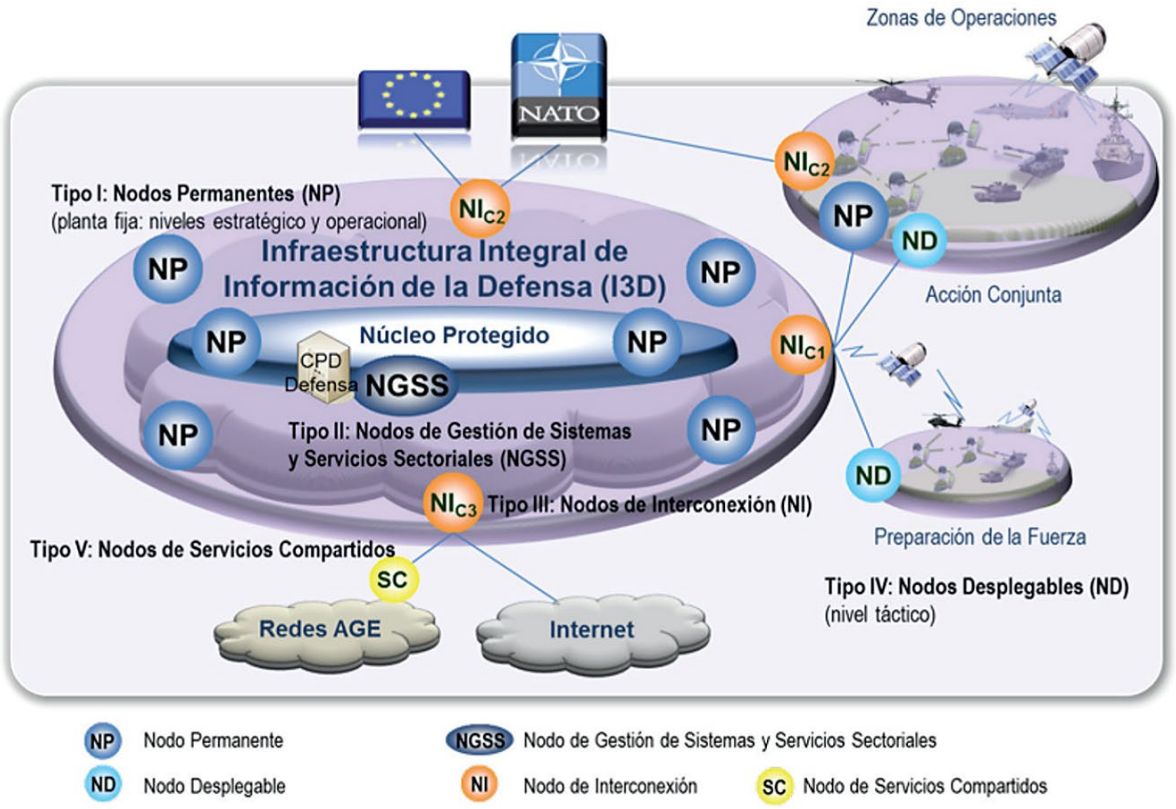

Figura 1. Esquema de la Infraestructura Integrada de Información de la Defensa (I3D). *Fuente: Ministerio de Defensa*

tecnologías no pueden desarrollar todo su potencial sino van acompañadas de una transformación digital completa, es decir, de un cambio en la cultura y la organización para adaptarse a las nuevas formas de trabajo. Este concepto de Tecnologías 4.0 también tiene su reflejo en el ámbito militar, donde se están desarrollando iniciativas como la Base Logística del Ejército, la Base Aérea Conectada, Sostenible e Inteligente (BACSI) o el Arsenal del futuro.

También es importante destacar que nos encontramos en una situación nueva en el mundo de la tecnología, ya que los últimos avances en muchas de ellas se encuentran en las empresas civiles, en lugar de en los centros de investigación o las universidades. La aplicabilidad al ámbito militar suele estar más enfocada al desarrollo de conceptos de empleo, o a su implementación en aplicaciones concretas, que en el propio desarrollo de la tecnología. Esta situación contrasta con gran parte de las tecnologías de la defensa, donde la especificidad de sus requisitos suele demandar desarrollos propios. Es decir, que las empresas del sector de la defensa deben orientar sus esfuerzos, en su gran parte, a la vigilancia tecnológica y a la búsqueda de aplicaciones y modos de incorporarlas a la Defensa.

Una de las consecuencias de esta situación es que el acceso a estas tecnologías es mucho más fácil y abierto a muchos actores, de modo que se reduce la ventaja militar que proporcionaban, tradicionalmente, las tecnologías desarrolladas dentro del sector de la Defensa.

Adoptar estos avances también ha generado una altísima dependencia y muchos riesgos

Por otro lado, la alta velocidad de desarrollo y fácil acceso hacen que no se pueden manejar de la misma manera que otras tecnologías. Es necesarios desarrollar unos procedimientos ágiles, que permitan unos tiempos de adopción más reducidos. Así, por ejemplo, el Departamento de Defensa de los Estados Unidos, dentro de su estrategia de modernización digital, establece como uno de sus objetivos "mejorar los procesos de implementación rápida de tecnologías", de modo que reconoce que los procesos de adquisición existentes suponían un problema para la adopción de estas tecnologías en los tiempos adecuados. Otro ejemplo que podemos ver en dicho documento, más enfocado en una tecnología concreta, pero en la misma línea, es la creación de un centro conjunto de Inteligencia Artificial (IA), que permita acelerar la adopción e integración de las capacidades basadas en la IA.

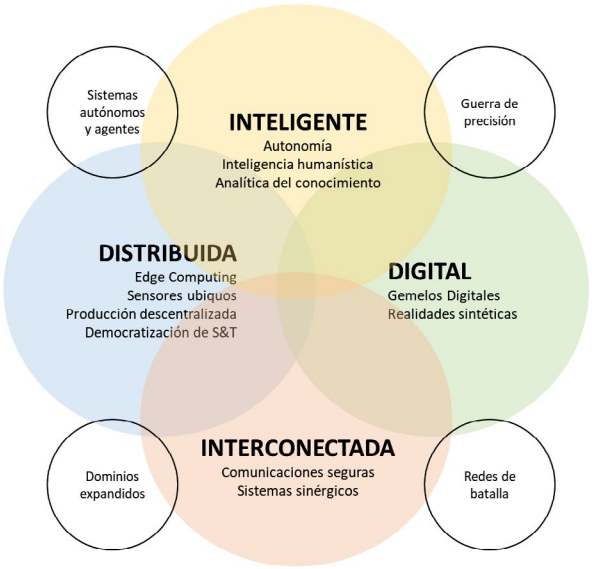

Figura 2. Tecnologías I2D2. *Fuente: Adaptado de NATO Science & Technology Trends 2020-2040*

A la hora de analizar las TIC en el ámbito del Ministerio de Defensa podemos considerar dos ámbitos bien diferenciados: el del propósito general y el relacionado con las capacidades militares. El ámbito de propósito general abarca todo el conjunto de plataformas y sistemas relacionados con la gestión administrativa, mientras que el de las capacidades militares abarca las relacionadas con las operaciones militares de las fuerzas armadas. Se trata, no obstante, de una separación artificial, ya que existe una gran relación entre ambos en muchas aplicaciones. El ministerio ha establecido una red común que da soporte a ambos ámbitos, la Infraestructura Integral de Información de Defensa (I3D), que permite ofrecer todos los servicios de comunicación demandados tanto por el Ministerio de Defensa como por las Fuerzas Armadas.

Los últimos avances se encuentran en muchas ocasiones en las empresas, en vez de en los centros de investigación

En el ámbito militar, los sistemas de información y comunicación (CIS), en todo su espectro, constituyen una parte fundamental de lo que se conoce como capacitadores conjuntos. En general, se trata de tecnologías que permiten la obtención, protección, difusión, análisis y explotación de los datos.

Históricamente, los sistemas de armas carecían de una componente TIC tan acusada. Sin embargo, en la actualidad se encuentran mucho más sensorizados y conectados, y previsiblemente esta tendencia se incrementará en el futuro. Esto va a permitir obtener una gran cantidad de datos que es necesario distribuir, almacenar y procesar adecuadamente para obtener inteligencia de ellos. No hablamos solo de datos externos al sistema de armas, que permiten obtener conciencia situacional e información del campo de batalla, sino de datos internos del propio funcionamiento del sistema, enfocados a optimizar su empleo y sostenimiento.

Tal y como se establece en el documento de tendencias 2020-2040 de la Organización de Ciencia y Tecnología de la OTAN (STO), las tecnologías que van a definir el futuro de la defensa tienen una naturaleza inteligente, interconectada, distribuida y digital (I2D2). Estas cuatro características, vinculadas cada una de ellas a diferentes tecnologías, permiten dibujar un escenario donde emergen algunas de las principales tendencias dentro del campo de batalla que serán claves para asegurar la superioridad en los futuros conflictos en los que se vean involucradas nuestras Fuerzas Armadas. Entre ellos, tal y como identifica el documento de tecnologías de la OTAN, figuran los sistemas autónomos e inteligentes, la guerra de precisión, las redes de batalla y los dominios expandidos.

3. Tendencias tecnológicas

Dentro de la labor de vigilancia tecnológica, casi todos los ministerios de Defensa y organizaciones están elaborando estrategias y realizando prospectivas sobre las tecnologías TIC existentes, y sobre cuáles pueden ser sus aplicaciones y sus impactos en la defensa. Si bien existen muchas tecnologías candidatas, existe bastante consenso en que hay un grupo de ellas que van a contribuir a definir el futuro de la defensa y que pueden contribuir a mantener o alcanzar una superioridad tecnológica que se traduzca en superioridad militar. A continuación se recogen algunas de las tecnologías identificadas por muchos de los ministerios de Defensa como claves para el futuro. Aunque el listado no es exhaustivo y se podrían incluir más tecnologías, nos vamos a centrar en aquellas que aparecen recurrentemente en documentos de referencia del Departamento de Defensa de Estados Unidos o de la OTAN.

3.1. INTELIGENCIA ARTIFICIAL

Se trata de tecnologías capaces de analizar grandes cantidades de datos buscando patrones, con menores tiempos de reacción, apoyando así a la toma de decisiones. Estas capacidades pueden dar lugar a nuevos conceptos de operación, como son el uso de enjambres de drones. Esta tecnología también está detrás de la automatización de los sistemas, permitiendo su operación de manera autónoma o bien descargando a los operadores de algunas de las tareas más repetitivas o monótonas, y permitiéndoles así concentrase en aquellas donde puedan aportar más valor.

3.2. TECNOLOGÍAS CUÁNTICAS

Aquí podríamos incluir tanto la computación, como las comunicaciones o los sensores cuánticos. Si bien se trata de tecnologías aun en desarrollo y cuyas aplicaciones por el momento son limitadas, ofrecen una gran perspectiva de futuro. La computación cuántica supone un cambio de paradigma computacional que va a revolucionar ámbitos como la simulación, los problemas de optimización y la criptografía. Las comunicaciones cuánticas, basadas en fenómenos cuánticos como el entrelazamiento o la superposición, van a permitir comunicaciones seguras, ya que es posible detectar cuando los mensajes han sido interceptados. Por último, los sensores cuánticos van a potenciar las aplicaciones ISTAR gracias a su gran sensibilidad, su bajo consumo y la superior resistencia a las perturbaciones (*jamming*).

3.3. REDES 5G

Las redes de quinta generación van a ser claves a la hora de manejar el gran volumen de dispositivos conectados y de datos transmitidos. Se trata de redes con velocidades de transmisión próximas a la de la fibra óptica y tiempos de latencia (tiempo de respuesta de los dispositivos) muy reducidos. La importancia de estas redes se ilustra en el veto establecido por el Gobierno de los EEUU a las empresas chinas a la hora de suministrar equipos para su red de 5G debido a su carácter estratégico.x

3.4. INTERNET DE LAS COSAS (IOT –INTERNET OF THINGS)

Se trata de un concepto que describe a objetos cotidianos sensorizados y con capacidad de comunicación que se conectan entre sí mediante una red. A nivel militar, esta conectividad ofrece una conciencia situacional mucho más amplia, ya que permite conocer el estado tanto de sistemas de armas (aviones, buques, drones, vehículos, etc.) como del propio equipamiento del soldado (armamento, dispositivos biométricos, etc.), así como de múltiples sensores del campo de batalla.

Toda esta información, debidamente procesada, permite obtener inteligencia tanto para la toma de decisiones en el campo de batalla, como para la logística o mantenimiento y operación óptimas de los sistemas de armas.

A esta aplicación del IoT al ámbito militar se le denomina como IoMT/IoBT (Internet of Military/Battlefield Things). En Estados Unidos existe una alianza entre el Gobierno, la industria y universidades para promover la aplicación de los desarrollos civiles a este campo.

3.5. ZERO TRUST SECURITY

Se trata de un nuevo paradigma de seguridad de redes para el que solo se considera confiable al usuario y el dispositivo que ha sido verificado. Este enfoque contrasta con la seguridad tradicional, orientada a prevenir accesos no autorizados desde el exterior y que considera como confiable todo acceso desde el interior de la red. Debido a las características de este enfoque, su empleo está más recomendado para aquellos ámbitos donde la información sea más crítica o donde la sensibilidad a los riesgos sea mayor.

3.6. DESARROLLO, SEGURIDAD Y OPERACIONES (DEV SEC OPS – DEVELPMENT, SECURITY, OPERATIONS–)

Más que de una tecnología se trata de una metodología consistente en incorporar la seguridad a lo largo de todo el ciclo de vida, empezando por la fase de desarrollo del software y de la infraestructura. Los ciclos de desarrollo son cada vez más cortos y, como hemos visto, la necesidad de seguridad es cada vez mayor, por lo resulta imprescindible adoptar estos enfoques, al objeto de minimizar las vulnerabilidades en los sistemas que puedan suponer brechas en su seguridad y en la de los datos que manejan.

3.7. DISPOSITIVOS DEFINIDOS POR SOFTWARE

Se trata de tecnologías donde una serie de componentes que tradicionalmente se implementaban mediante hardware han pasado a ser implementados mediante software. Podemos hablar aquí, por ejemplo, de las radios definidas por software (Software

Defined Radio –SDR–) o de las redes definidas por software (Software Defined Networks –SDN–). Al no estar limitados por la rigidez del hardware, estos dispositivos son más fáciles de escalar, gestionar, actualizar o modificar sus funcionalidades, ya que no requieren rediseños y sustitución de los componentes. Solo basta con modificar el software.

3.8. BIG DATA Y ANALÍTICA AVANZADA

Como surge de muchas de las tecnologías antes mencionadas, la adecuada gestión de los datos es una de las claves tanto en el presente como en el fututo de las TIC. Cada vez tenemos que manejar un mayor volumen de datos y además de fuentes distintas. Ya no se trata del simple manejo de datos estructurados, sino que hay que procesar imágenes, información de redes sociales, audios, sensores, etc. El Big Data y la analítica avanzada son un conjunto de tecnologías que permiten recolectar los datos, almacenarlos, comunicarlos y analizarlos, apoyando así la toma de decisiones. Las características de estas tecnologías se suelen resumir bajo las denominadas 5 V, que hacen referencia al tipo y forma de manejar los datos: volumen, velocidad, variedad, veracidad y visualización. Tal y como recoge el documento Science & Technology Trends 2020-2040, el reto del Big Data y la Analítica Avanzada es "dar sentido a grandes cantidades de datos no homogéneos que llegan muy rápido y cuya precisión y autenticidad es potencialmente dudosa".

Muchas de estas tecnologías, presentadas aquí de manera separada, configuran un paisaje conjunto donde se entrelazan y se hacen clave las unas para las otras. Cuanto mayor es el volumen de datos y más se recurre su almacenamiento y procesado en la nube, tanto pública como privada o hibrida, mayor es la necesidad de una alta velocidad de transmisión (redes 5G), de protección de dichos datos (Zero Trust Security) o de análisis (Big Data o inteligencia artificial).

3.9. TECNOLOGÍAS DE COMPUTACIÓN EN LA NUBE

Cabe hacer una mención especial a las denominadas tecnologías cloud, o de almacenamiento y computación en la nube. La migración a la nube es una tendencia clara en el mundo de las TIC, ya que facilita el acceso a los datos, facilita su seguridad e incluso permite una reducción de costes. Para eso las organizaciones tiene la posibilidad de recurrir a nubes públicas o privadas, cada una con sus ventajas e inconvenientes. Sin embargo, últimamente está ganado fuerza un modelo mixto, que combina nubes privadas con nubes públicas, e incluso con sistemas *On Premise*. La clave es que estos sistemas sean capaces de orquestar el funcionamiento de todas ellas de manera ágil, de modo que permitan que funcionen como una única entidad, trasladando fácilmente la carga de trabajo y los datos entre ellas y facilitando su gestión.

A pesar de los avances a la hora de establecer infraestructuras de telecomunicación que den un adecuado soporte a las operaciones militares, siguen existiendo entornos operacionales donde el acceso a estas infraestructuras es limitado o directamente nulo. Para solventar estos problemas se están desarrollando e implementando tecnologías de computación fronteriza (*Edge Computing*). La computación fronteriza consiste en llevar la capacidad de almacenamiento y procesado de la información al entorno donde es demandada, en lugar de tener que recurrir a infraestructuras remotas como la nube. Sistemas como el avión de combate de quinta generación F-35 son capaces de recibir, integrar y procesar información de múltiples sensores para luego distribuirla a otros sistemas dentro de la zona de operaciones. Otra ventaja de esta tecno-

logía es que permite mantener cierta información crítica dentro de un área controlada, en lugar de enviarla a grandes centros de datos donde puedan colarse accesos no autorizados.

En la convergencia entre ambos mundos ha surgido otro concepto que esta ganando mucha fuerza: la nube de combate (*Combat Cloud*) o nube de combate multidominio (Multi-Domain Combat Cloud –MDCC–). Se trata de sistemas descentralizados que integran la información de múltiples nodos a lo largo de todos los dominios (tanto los tradicionales de tierra, aire y mar como los nuevos de espacio y ciber) utilizando tecnologías basadas en la nube, y que permiten extender su operación a entornos donde el acceso a esta infraestructura sea más limitado.

3.10. CIBERSEGURIDAD

Aunque no se trata de una tecnología en sí misma, no cabe duda de que constituye una capacidad imprescindible y transversal a todo el resto de las tecnologías antes comentadas. Las tendencias actuales en el mundo de las TIC configuran un escenario donde aumenta exponencialmente la demanda de servicios conectados (servicios en la nube, tecnologías 5G, IoT, etc.). Esta dependencia creciente aumenta las vulnerabilidades que pueden ser explotadas por los atacantes y que es necesario proteger, hasta el punto de haber dado lugar a un nuevo dominio operativo, el ciberespacio.

A nivel gubernamental, en 2022 se ha publicado un nuevo Esquema Nacional de Seguridad (ENS), el cual busca reforzar las capacidades de defensa ante ciberamenazas sobre el sector público, incorporando, entre otras, medidas de seguridad relativas a servicios en la nube, la interconexión de sistemas o la protección de dispositivos conectados a la red.

De la necesidad de avanzar en las capacidades de este nuevo dominio se hace también eco la propia Estrategia de Tecnología e Innovación de la Defensa (ETID), en la cual se han identificado una seria de retos tecnológicos para los cuales se han definido objetivos tecnológicos, como el de Soluciones para ciberoperaciones, así como líneas de I+D+i agrupadas en la subárea 11.4 Seguridad de Sistemas e Información. Estas líneas abarcan tanto defensa (automatización de acciones ante ciberataques, análisis predictivo de vulnerabilidades y dispositivos criptológicos) como la respuesta a los ataques (apoyo a ciberoperaciones).

Algunas de las tendencias tecnológicas analizadas en este dossier también se derivan de la necesidad de proteger los sistemas TIC, como son el esquema de Zero Trust o la metodología DevSecOps.

4. Iniciativas europeas

El plan de acción sobre sinergias entre industrias civiles, defensa y espacio aprobado en 2021 por la Comisión Europea contempla al sector electrónico y digital como uno de los más relevantes sobre los que aplicar políticas y programas que mejoren la eficiencia y potencien la capacidad europea en tecnologías relacionadas con este sector. Posteriormente, la actualización de la estrategia industrial de la UE, incide en la importancia de políticas y programas que incentiven la transformación digital para potenciar la recuperación económica europea.

En el ámbito específico de la defensa, la propia Comisión aprobó en febrero de 2022 un documento de concepto donde se planteaban medidas para

mejorar las capacidades de la UE ante las amenazas del actual entorno estratégico, en donde las TIC juegan un papel determinante y en donde se trata de forma amplia las amenazas híbridas, especialmente las relacionadas con el ciberespacio. El documento estaba acompañado por una hoja de ruta donde se señalan acciones e iniciativas para mejorar la situación en cuanto a tecnologías críticas para la seguridad y la defensa.

El ámbito de las tecnologías críticas ha sido uno de los prioritarios en los que propiciar la colaboración entre los estados miembros de la UE. En el ámbito Pesco se están desarrollando diez iniciativas relacionadas con ciberespacio y mando y control, lo que representa un 15% del total de iniciativas aprobadas. Las relacionadas con otras áreas de actividad tienen en su mayoría un componente TIC elevado.

En el ámbito del EDAP (Plan de Acción Europeo para la Defensa), tanto en la iniciativa EDIDP (Programa Europeo de Desarrollo Industrial en Materia de Defensa) como los EDF (Fondos Europeos de Defensa) como consecuencia de las convocatorias resueltas hasta la fecha, se han aprobado un total de 25 proyectos relacionados con TIC y ciberseguridad, que movilizan un total por encima de los 300 millones de euros, de los que aproximadamente el 90% son aportaciones procedentes de fondos comunitarios, y suponen la cuarta parte del total de proyectos aprobados.

En este ámbito, la perspectiva para los próximos años para el EDF en las categorías relacionadas con superioridad de la información, ciber o transformación digital podrían llegar a concentrar entre un 30 y un 40% del total de la financiación disponible. Entre otras los resultados que se esperan de estas inversiones son la mejora de las capacidades en:

- C2 a nivel operacional y para operaciones especiales.
- Interoperabilidad en comunicaciones tácticas.
- Operaciones en ciberespacio.
- Nube de combate.
- Inteligencia artificial.
- Tecnologías cuánticas.

Cuadro 1. Iniciativas Pesco relacionadas con ámbito C2 y Ciber

PROYECTO	DESCRIPCIÓN	LIDER	PARTICIPANTES
ESSOR	Software defined radio	FRANCIA	ALEMANIA, BELGICA, ESPAÑA, FINLANDIA, HOLANDA, ITALIA, POLONIA, PORTUGAL
CTISP	Cyber threats and incident response platform	GRECIA	CHIPRE, HUNGRÍA, ITALIA, PORTUGAL
CRRT	Cyber rapid response teams	LITUANIA	CROACIA, ESTONIA, HOLANDA, POLONIA, RUMANIA
EUMILCOM	Strategic C2 system	ESPAÑA	ALEMANIA, FRANCIA, ITALIA, LUXEMBURGO, PORTUGAL
EHAAP	European high atmosphere airship platform	ITALIA	FRANCIA
SOF C2 CP	SOF tactical C2 CP for small joint operations	GRECIA	CHIPRE
EWC	EW capability for future JISR	CHEQUIA	ALEMANIA
CIDCC	Cyber domain coordination center	ALEMANIA	FRANCIA, HOLANDA, HUNGRÍA
CRF	Cyber range federations	ESTONIA	BULGARIA, FINLANDIA, FRANCIA, LETONIA, ITALIA, LUXEMBURGO
AMIDA UT	Automated modelling and damage assesment for urban terrain	PORTUGAL	ESPAÑA, FRANCIA

Cuadro 2. Proyectos seleccionados en convocatorias EDIDP relacionados con TIC y ciberseguridad

EDIDP 2019

PROYECTO	DENOMINACIÓN	MESES	ACTIVIDADES	TOTAL €	UE €	% UE
ECYSAP	Cyber situational awareness platform	48	Study, design, prototyping, testing and qualification	18.855.619,00	10.920.133,00	57,91
ESC2	European C2 system	30	Study, design	21.999.961,00	20.000.000,00	90,91
PANDORA	Cyber defence platform for real time threat hunting, incident response and information sharing	24	Study, design, prototyping and testing	7.632.434,00	6.813.995,00	89,27
PEONEER	Persistent Earth observation for actionable ISR	36	Study, design, prototyping and testing	8.481.137,00	7.253.304,00	85,52
SMOTANET	Development of software defined mobile ad-hoc tactical network devices and testbed	36	Study, design	3.907.724,00	3.907.724,00	100,00

EDIDP 2020

PROYECTO	DENOMINACIÓN	MESES	ACTIVIDADES	TOTAL €	UE €	% UE
AI4DEF	Artificial intelligence for defence	36	Study, design, prototyping and testing	7.089.429,55	5.699.954,71	80,40
CYBER4DE	Cyber rapid response toolbox for defence use	30	Study, design, prototyping, testing, and qualification	9.685.754,42	9.325.122,72	96,28
DISCRETION	Disruptive SDN secure communications for european defence	42	Study, design, prototyping and testing	6.719.699,75	5.169.394,17	76,93
SIGNAL	Photonics based SIGINT payload for class II RPAS	30	Study, design, prototyping and testing	3.062.014,00	2.492.526,63	81,40

	COORDINA	ENTIDADES	PAISES	ESPAÑA	DESCRIPCIÓN
	ESPAÑA (INDRA)	9	4	INDRA (L), INNOTEC SYSTEM SL, S2 GRUPO, UNIVERSIDAD CIII, UPM, UPV	Cyber situtational awareness picture for military end users to become a real time defensive system capable of ciber response in the area of operations
	ESPAÑA (INDRA)	17	10	INDRA (L), GMV	Development of advance SC2 system fully interoperable with teh C2 systems from EU, member states, NATO and civilian ageWncies
	GRECIA (SPACE HELLAS)	15	8	CENTRO TECNOLOGICO DE TELECOMUNICACIONES DE CATALUÑA	Open technical solution for real time threat hunting and incident response
	ITALIA (E-GEOS)	10	8	ATEM NUEVAS TECNOLOGIAS, HISDESAT	Software platform to implement Activity Based Intelligence for geo spatial activities
	GRECIA (INTRACOM)	5	3	CROACIA, ESTONIA, HOLANDA, POLONIA, RUMANIA	To design a modular, adaptive and secure tactical network

	COORDINA	ENTIDADES	PAISES	ESPAÑA	DESCRIPCIÓN
	DINAMARCA (TERMA)	19	10	GMV	To demonstrate the benefits of Artificial intelligence on military functional areas
	LITUANIA (BALTIJOS TECHNOLOGIJU INSTITUTAS)	10	7		Ciber toolbox for defence aiming to enhance processess and practices of cyber response teams
	PORTUGAL (DEIMOS ENGENHARIA)	9	4	Telefonica / UPM	To develop an optical software defined network solution for secure communications
	ESPAÑA (DAS PHOTONICS)	3	3	DAS PHOTONICS (L)	To develop payloads to improve resilience in complex or saturated electromagnetic environments to be installed in small platforms such as tactical drones

Cuadro 3. Proyectos seleccionados en convocatorias EDF relacionados con TIC y ciberseguridad

EDF 2021

PROYECTO	DENOMINACIÓN	MESES	ACTIVIDADES	TOTAL €	UE €	% UE
5G COMPAD	5G communications for peacekeeping and defense	36	Studies, design, prototyping, testing	37.096.363,98	26.998.532,29	72,78
ACTING	Advanced european platform and network of cybersecurity training and exercises centres	48	Studies, design, prototyping, testing	17.784.582,50	16.258.054,13	91,42
ADEQUADE	Advanced, disruptive and emerging quantum technologies for defence	36	Studies, design	27.433.831,28	27.433.831,28	100,00
AGAMI	European innovative GaN advanced microwave integration	48	Studies, design	24.555.323,82	24.555.323,82	100,00
AINCEPTION	AI framework for cyber defence operations	36	Studies, design	8.147.875,50	8.147.875,50	100,00
ALADAN	AI based language technology development framework for defence applications	42	Studies, design, prototyping,	3.235.279,56	3.143.675,82	97,17
EDOCC	European Defence Operational Collaborative Cloud	36	Studies, design	42.252.208,51	40.000.000,00	94,67
EU GUARDIAN	Framework and proofs of concept for the intelligent automation of cyber defence incident management	36	Studies, design	13.454.545,33	13.454.545,33	100,00
FARADAI	Frugal and robust AI for defence advanced intelligence	42	Studies	18.498.239,16	18.498.239,16	100,00
FIBER SAFE	Developing the world´s first radio over fibre modular deployment system	34	Studies, design, prototyping	3.307.317,82	2.405.026,40	72,72
HEGAPS	Hybrid energy grid and propulsion system	24	Studies, design	3.998.363,25	3.998.363,25	100,00
HIDRA	High instantaneous dynamic range direct RF sampling modular chiplet architecture	36	Studies, design	3.996.992,42	3.996.992,42	100,00
KOIOS	Knowledge extraction, machine learning and other AI approaches for se cure robust, frugal, resilient and explainable solutions in defence applications	36	Studies	9.989.713,00	9.989.713,00	100,00
POWERFLEX	Smart heterogeneous technological platform extending the power and frequency limits of flexible nanoelectrics	36	Studies, design	3.458.087,24	3.458.087,24	100,00
POWERPACK	Novel 3D heterogeneous integration for future miniaturized power RF transceiver front ends	36	Studies, design	3.494.531,61	3.494.531,61	100,00
SMIEQ	Secure microcontroller with embedded quantum random number generator	42	Studies, design	3.559.716,13	3.494.090,26	98,16

	COORDINA	ENTIDADES	PAISES	ESPAÑA	DESCRIPCIÓN
	SWE (SAAB)	19	12	INSTER	To demonstrate the relevance of 5G mobile communications technology in support of sustained information superiority
	BUL (INSTITUT PO OTBRANA)	28	13	MANAGING AND INNOVATION, TELEFÓNICA MÓVILES	To develop advanced interconnected domain oriented cyber ranges for training and exercises
	FRA (THALES)	31	8	INDRA, SENER, INSTITUTO CIENCIAS FOTÓNICAS	To provide a breakthrough in quantum-sensing domains to develop capabilities with technological, operational and strategic advantages in different areas
	DEU (UNITED MONOLITIC)	34	12	AIRBUS, INDRA, U. DE VIGO, UPM	GaN integration for radar and electronic warfare
	GRE (SPACE HELLAS)	18	9		To improve cyber defence operations by using AI based tools and techniques
	FRA (VOCAPIA)	4	4		AI based language solutions for defence applications that will rely mainly on the use of non confidential data
	DEU (ADS)	26	11	E4 COMPUTER ENGINEERING, GMV, INDRA, NAVANTIA, THALES PROGRAMAS	To provide a virtual platform to increase collaborative services on the battlefield
	ESP (INDRA)	10	7	INDRA (L), U. DE MURCIA	To create an AI based solution to automate incident management and cyber defence processes
	GRE (CERTH)	35	13	INDRA, TECNALIA, THALES PROGRAMAS, UPM	To develop AI for defence applications based on frugal learning (ability of a system to adapt and learn from its environment)
	SWE (Mircropol Fiberoptic)	3	3		To develop a modular high bandwith radio frequency over fibre (RFOF) for military communications
	ESP (Seaplace)	7	4	SEAPLACE (L), EDAIR, SUPRASYS, FUNDACIÓN CENTRO TECNOLOGÍAS AERONAUTICAS	Cyber physical system to coordinate multiple assets into an integrated naval grid. Digital twin environment to coordinate different assets by digital simulation of multiagent systems
	SLO (Beyond semiconductor)	4	3		Studies and design regarding digital signal processing for SDR
	ESP (CT Ingenieros)	14	8	CT INGENIEROS (L), NTT DATA SPAIN, MITIGA SOLUTIONS, CENTRO NACIONAL DE SUPERCOMPUTACIÓN	To improve AI for military applicatons, spanning simulation, use-cases, metrics and real world experiments
	FRA (THALES)	10	6		New flexible antennas based on new and advanced materials
	FRA (THALES)	10	6	CIDETE INGENIEROS	To develop miniaturized RF chips for high frequency and high power operation
	FRA (BULL)	3	2		Secure microcontroller with embedded quantum random number generator for protection of weapon systems against cyber attacks

5. Estrategia de tecnología e innovación para la defensa (ETID)

En el Ministerio de Defensa español, al amparo de la I3D y del Plan Estratégico de los Sistemas y Tecnologías de la Información y las Comunicaciones del Ministerio de Defensa (Pecis), se están aprobando estrategias específicas para redes 5G o la explotación de la nube. Por su puesto que estas no son las únicas tecnologías TIC de importancia para la defensa, aunque sí que puede que sean algunas de las más importantes o en las que se está poniendo más el foco. No obstante, podríamos mencionar otras, como las redes ópticas pasivas, la hiperconvergencia, el IPv6 y la criptografía avanzada, por ejemplo.

Para poder aprovechar el potencial de todas estas tecnologías es necesario que tanto las empresas como los gobiernos se enfoquen en su vigilancia y desarrollo. A nivel del Ministerio de Defensa, una de las principales herramientas desarrolladas para este fin es la Estrategia de Tecnología e Innovación para la Defensa (ETID), donde se definen una serie de líneas de I+D+i de interés para la defensa, las cuales prioriza mediante unos objetivos tecnológicos agrupados en tres niveles. En su edición de 2020, la ETID define 11 líneas tecnológicas, una de las cuales se centra específicamente en las tecnologías de la información, comunicaciones y simulación. No obstante, la importancia de este tipo de tecnologías es tal que impregna muchas de las otras líneas de I+D+i. Así, podemos encontrar tecnologías relacionadas con las TIC en las líneas, de sensores y sistemas electrónicos, sistemas espaciales, o incluso en las de los diversos tipos de plataformas. Con respecto a los objetivos tecnológicos, podemos destacar los relacionados con la inteligencia artificial o la simulación, o con las tecnologías 4.0 para la modernización de departamento, dentro del nivel de desarrollo de tecnologías para los principales desafíos y retos tecnológicos de defensa. Para el nivel de tecnologías avanzadas para las futuras grandes plataformas y sistemas de armas de defensa, si bien se trata de un nivel muy abierto, incluye como ejemplo algunas de las tecnologías que se están desarrollando para el FCAS (Future Combat Air System), dentro las cuales podríamos destacar la nube de combate, los sensores avanzados o la simulación. Por último, en el nivel de tecnologías emergentes, el documento apunta principalmente a las tecnologías cuánticas (computación, comunicación, información, sensores y simulación).

La actual situación de incertidumbre refuerza aún más la necesidad de colaboración entre los mundos militar y civil

Como se expuso con anterioridad, algunas de estas tecnologías están lideradas por empresas. La propia ETID se hace eco de esta realidad y por eso uno de los ámbitos de actuación, dentro del nivel de desarrollo de tecnologías para los principales desafíos y retos tecnológicos de defensa, es el de aprovechamiento del empuje tecnológico civil.

Las actividades de logística distributiva y de campaña se enfrentan al desafío de incorporar las posibilidades de las nuevas tecnologías para dar una mejor respuesta en un entorno complejo desde el

punto de vista geoeconómico. Al entorno ya complicado al que se enfrentaban por la covid, se añade ahora la situación provocada por la invasión de Ucrania. Esta situación de incertidumbre refuerza aún más la necesidad de colaboración entre los mundos militar y civil para poder afrontar las diferentes situaciones con garantías de éxito mutualizando capacidades.

La coordinación de las capacidades orgánicas militares con las que aporta el sector empresarial proporciona robustez y fortaleza. Es quizá una coordinación más necesaria que nunca para proporcionar eficacia y eficiencia en el servicio prestado, junto a la necesidad de establecer mecanismos para intercambiar conocimientos, prácticas e ideas. En este ámbito, la experiencia de las empresas de Aesmide resulta muy útil para estar en vanguardia en el campo estratégico que es la logística.

6. El apoyo empresarial. Capacidades de Aesmide

Este empuje desde el ámbito civil se manifiesta claramente en conjunto de la oferta que proporcionan las empresas de Aesmide en estas tecnologías y que cubre toda la gama de necesidades. Su ámbito de actividad se puede agrupar en tres grandes bloques: consultoría y servicios, servicios asociados a infraestructura, y equipos de comunicaciones. Es difícil categorizar a las empresas en exclusiva dentro de un bloque concreto, puesto que buena parte de ellas proporcionan servicios de forma transversal y además actúan en otros ámbitos especialmente en ciberseguridad. En términos de empleo, su impacto en el mercado laboral español es importante, puesto que generan alrededor de 170.000 puestos de trabajo directos en España.

Las empresas de Aesmide en estas tecnologías generan alrededor de 170.000 puestos de trabajo directos en España

TELEFÓNICA engloba a aproximadamente el 70% de esos 140.000 profesionales. Este gran grupo multinacional español factura unos 50.000 millones, de euros anuales de los que aproximadamente tres cuartas partes proceden de su actividad en el exterior. Mayoritariamente, su actividad se realiza en el sector de comunicaciones civiles, aunque opera también en el sector de seguridad y defensa. Sus actividades en apoyo del Ministerio de Defensa español son muy significativas. Proporciona servicios e infraestructuras de datos, telefonía, acceso a internet y telemedicina en el marco del proyecto I3D. En el ámbito de seguridad, en marzo de este año fue seleccionada, junto con Indra, por el Ministerio de Transformación Digital para la construcción del nuevo Centro de Operaciones de Ciberseguridad de la Administración General del Estado y Organismos Públicos (COCS). En cuanto a servicios con aplicaciones duales, en julio de 2022 se ha aliado con Sateliot para proporcionar nuevos servicios de conectividad 5G en zonas no conectadas hasta el momento, en apoyo de sectores como la agricultura, la ganadería o las instalaciones de generación de energías renovables. En el ámbito europeo, participa en el marco EDIDP en el proyecto Discretion para el desarrollo de soluciones innovadoras de comunicaciones tácticas seguras. En el marco

EDF cabe destacar la participación de Telefónica Móviles en el proyecto Acting, en el que participan 28 empresas de 13 países y que será financiado por la Comisión Europea con más de 16 millones de euros para el diseño de una red europea avanzada para formación y ejercicios en el ámbito de la ciberseguridad.

El resto de empresas integradas en Aesmide que desarrollan su actividad en el sector TIC facturan en global en España una cifra próxima a los 2.000 millones de euros anuales, también mayoritariamente en el ámbito civil. Su presencia en el ámbito de defensa y seguridad tiene relativamente poco peso para el conjunto de su actividad, pero proporcionan servicios esenciales para los Ministerios de Defensa e Interior españoles. El segmento está conformado por la presencia de grandes grupos internacionales o europeos, y un número de pymes de capital español con una capacitación tecnológica de primer nivel.

6.1. CONSULTORÍA Y SERVICIOS

ALTRAN se integró en Capgemini Engineering en abril de 2020. Desde su creación hace más de 30 años se ha convertido en una referencia en la provisión de servicios de ingeniería y tecnología relacionados principalmente con movilidad urbana, ferrocarriles del futuro y el sector aeroespacial. En este último campo, ha desarrollado sistemas de preparación de misiones para aviación de combate. Capgemini es líder mundial en servicios de transformación digital.

CITRIX SYSTEMS SPAIN es filial del grupo norteamericano Citrix, líder mundial en tecnologías de trabajo digital. Proporciona soluciones que permiten a los usuarios trabajar en la nube o en instalaciones desde cualquier plataforma o dispositivo en condiciones seguras y con facilidad de acceso.

FUTURESPACE es una empresa con más de 20 años de experiencia especializada en el desarrollo de productos y soluciones software para la mejora de procesos de negocio e inteligencia económica. En el ámbito de la seguridad y la defensa está especializada en el desarrollo de plataformas de inteligencia e investigación.

El grupo multinacional **INETUM** adquirió en 2019 lecisa. Desde entonces ha consolidado su presencia en España como socio de referencia con diferentes clientes, tanto públicos como privados. En el ámbito de la defensa y seguridad ha sido adjudicataria de contratos para modernizar el sistema de gestión logística del Ejército del Aire, los servicios de operación del Centro de Vigilancia y Operaciones de la Armada y mantenimiento del SIVE para la Guardia Civil.

INIXA inició su actividad hace alrededor de 20 años como un spin-off de la Universidad de Oviedo, y desde entonces se ha especializado en la provisión de servicios de ciberseguridad, criptografía e inteligencia. Su gama de productos CryptoX ofrece soluciones que cubren el ciclo completo de confidencialidad, integridad, disponibilidad, trazabilidad y autoría de datos e información.

NETCHEK es una empresa con más de 20 años de experiencia que proporciona servicios de consultoría en diferentes áreas de actividad. Recientemente está impulsando su actividad en procesos logísticos para proporcionar mayor agilidad, eficacia y seguridad para prevenir contingencias en operaciones logísticas y mejorar la eficiencia de la actuación de toda la cadena de suministro.

El gran grupo multinacional **ORACLE** cuenta con casi 1.400 empleados en España. Entre sus ámbitos de especialización hay que destacar su oferta de servicios en la nube para grandes clientes. La demanda de este segmento de servicios ha experimentado un importante crecimiento en los últimos

meses, con un aumento de un 33% interanual entre abril y junio de 2022 y un volumen a nivel mundial superior a los 60.000millones de euros. Este incremento se debe fundamentalmente a una mayor demanda de análisis de grandes datos y aprendizaje automático.

SALESFORCE es una multinacional norteamericana líder mundial en servicios de gestión de relaciones con clientes a través de soluciones basadas en la nube, que permiten a cualquier organización disponer de una visión unificada de sus clientes desde una plataforma integrada.

SAP una multinacional alemana que es líder en Europa en desarrollo de software, proporciona soporte a empresas de todo tamaño mediante soluciones basadas en aprendizaje automático, internet de las cosas y analíticas avanzadas.

6.2. SERVICIOS ASOCIADOS A INFRAESTRUCTURAS

BESS GROUP (Beyond Soluciones y Servicios S.L.), con más de 15 años de experiencia, ofrece soluciones y servicios para cubrir toda la cadena de suministro. En abril de 2022 resultó adjudicataria de un acuerdo marco con la Armada española para proporcionar asistencia técnica en apoyo logístico por dos años prorrogables durante tres más. Entre sus productos destacan el software CMOS (Control Móvil de Stocks) para control de inventarios, y el sistema Nexo para gestión de la cadena de suministro, que cubre el ciclo logístico completo enlazando de forma ágil a proveedores y clientes.

COTESA, integrada en el grupo Tecopy desarrolla su actividad fundamentalmente proporcionando servicios de consultoría para la gestión del territorio mediante el uso de tecnologías de información geográfica.

La Estrategia de Tecnología e Innovación para la Defensa defina una serie de líneas de I+D+i de interés militar

ETRA (Electronic Trafic S.A.) es un grupo internacional, con más de 30 años de experiencia, especializado en soluciones tecnológicas avanzadas en movilidad, infraestructura y comunicaciones. Cuenta con una gran experiencia internacional, con presencia en España, Portugal, Colombia, México, Brasil, Bulgaria, Perú y Alemania. En el ámbito europeo cuenta con una gran experiencia en el programa Horizonte 2020, en el que participa en 29 actividades, de las que coordina nueve. En el ámbito de seguridad y defensa, a finales de junio de 2022 presentó el caso Emergencias 4.0 en un puesto de mando avanzado para la gestión de emergencias, proporcionando capacidades de coordinación de sistemas dentro del proyecto piloto 5G de Red.es.

SISTEM, perteneciente al grupo CPS, es una empresa integradora de sistemas que ofrece a sus clientes soluciones globales, en los mercados del transporte inteligente, telecomunicaciones y seguridad, especializados en los sectores de tráfico, ferrocarriles y aeronaval. En el ámbito específico de seguridad portuaria ha diseñado la plataforma Hyperion como solución de seguridad integral abierta y modular, adaptable a cada puerto. Como empresa especializada en desarrollar soluciones de eficiencia energética, Sistem lidera el proyecto BrainEn para desarrollar una aplicación para el análisis y predicción de la generación y demanda de energía basada en inteligencia artificial. Dentro de la iniciativa eSmarcity ofrece soluciones para detectar, medir y analizar la situación en zonas de bajas emisiones a partir de algoritmos basados en inteligencia artificial.

Cuadro 4. Empresas TIC Aesmide

CONSULTORÍA Y SERVICIOS				
Capgemini engineering	**ALTRAN CAPGEMINI ENGINEERING**	C/ Campezo 1, 28022 MADRID	www.capgemini-engineering.com/	Análisis, diseño, producción y mantenimiento de sistemas. Transformación digital.
citrix	**CITRIX SYSTEMS SPAIN S.L.**	Pº de la Castellana 135, 28046 MADRID	www.citrix.com/	Desarrollo de soluciones TICs
FutureSpace	**FUTURESPACE**	Avenida Tenerife 2, 28073 SAN SEBASTIÁN DE LOS REYES (MADRID)	www.futurespace.es/	Desarrollo de soluciones software
iCOSMOS	**ICOSMOS**	4 Rue Michel Ange, 75006 Ile de France (PARIS - FRANCIA)	www.icosmoscorp.com/	Asesoría, servicios de software de gestión
inetum. Positive digital flow	**INETUM**	Travesía Costa Brava 4, 28034 MADRID	www.inetum.com/	Servicios y soluciones digitales. Desarrollo, integración y gestión de sistemas
INIXA	**INIXA**	C/ Fernández de Oviedo 36, 33012 OVIEDO	www.inixa.com/	Seguridad de la información, certificación digital y criptografía
NETCheck	**NETCHECK**	C/ Francisco Campos 22, 28022 MADRID	www.netcheck.es/	Big Data, Bussiness Intelligence e Inteligencia Artificial
ORACLE	**ORACLE**	Avda Jose Echegaray 6, 28230 LAS ROZAS (MADRID)	www.oracle.com/	Desarrollo de soluciones software
PRICE COST ESTIMATION SOLUTIONS	**PRICE SYSTEMS**	Price House Meridian, RG27 9HY HOOK HAMPSHIRE (UK)	www.pricesystems.com/	Soluciones en gestión de costes
salesforce	**SALESFORCE**	Paseo de la Castellana 79, 28046 MADRID	www.salesforce.com/	Gestión de relaciones con clientes (CRM)
SAP	**SAP**	C/ Torrelaguna 77, 28043 MADRID	www.sap.com/	Software de aplicaciones empresariales
Telefónica	**TELEFÓNICA**	Ronda de la Comunicación s/n, 28050 MADRID	www.telefonica.com/	Servicios completos de comunicaciones
EQUIPOS				
	GLOBAL RADIO SYSTEM	C/ Platino 1, 41909 SALTERAS (SEVILLA)	www.globalradiosystem.com/	Operador de radiocomunicaciones móviles
SERVICIOS ASOCIADOS A INFRAESTRUCTURA				
BeSS Group	**BESS GROUP**	C/ Oquendo 23, 28006 MADRID	www.beyondss.com/	Integración de cadenas de suministro.
cotesa	**COTESA**	C/ Luis Proust 17, 47151 BOECILLO (VALLADOLID)	www. cotesa.grupotecopy.es/	Tecnologías de información geográfica
etra	**ETRA (ELECTRONIC TRAFFIC S.A.)**	Avenida Tres Forques 147, 46014 VALENCIA	www.grupoetra.com/	Sistemas de gestión de transporte. Soluciones de seguridad
SISTEM	**SISTEM**	Avda Rita Levi Montalcini 2, 28906 GETAFE (MADRID)	www.sistem-group.com	Soluciones globales en transporte, telecomunicaciones y seguridad
S2 GRUPO	**S2 GRUPO**	C/ Ramiro de Maeztu 7, 46022 VALENCIA	www.s2grupo.es/	Souciones de ciberseguridad
TAISA	**TAISA**	Via de las Dos Castillas 33, 28224 POZUELO DE ALARCÓN (MADRID)	www.taisa.com/	Infraestructuras de comunicaciones
syvalue	**TAISA SYVALUE**	Avda. de la Victoria 23, 28023 MADRID	www.syvalue.com/	Infraestructuras de comunicaciones

S2 GRUPO ofrece desde hace más de 15 años servicios de ciberseguridad y ciberinteligencia con soluciones propias para detección y gestión de amenazas e incidentes, incluido el análisis forense y apoyo al diseño de estrategias de seguridad para operación de sistemas. En colaboración con el Ministerio de Industria, ha desarrollado el proyecto iHoney para mejorar la seguridad de sistemas de control industrial, y en colaboración con el CCN, ha desarrollado una solución para la detección de ataques denominada Carmen. Se trata de la única empresa de capital nacional en el sector que utiliza tecnología desarrollada completamente en España. Cuenta con una importante presencia en mercados internacionales, que representan aproximadamente el 25% de su facturación. En el ámbito EDIDP participa en el proyecto Ecysap para desarrollar soluciones de ciberseguridad en zonas de operaciones.

TAISA con una experiencia de más de 30 años de actividad se ha especializado en las infraestructuras de comunicaciones, especialmente de proceso de datos cuenta entre sus clientes con un buen número de Ministerios y organismos y entidades públicas.

TAISA-SYVALUE se creó en 2006 para la provisión de servicios de infraestructura informática. En UTE con Telefónica Soluciones suministra equipamiento para la infraestructura integral de comunicaciones e información del Ministerio de Defensa.

6.3. EQUIPOS

GLOBAL RADIO SYSTEM (GRS) lleva más de 20 años proporcionando soluciones de radiocomunicación a instituciones y empresas. GRS cuenta con presencia en España, Panamá, Chile, Reino Unido, Costa de Marfil, Uganda y Mozambique. Recientemente ha proporcionado equipos de comunicaciones portátiles a diferentes asociaciones que han suministrado ayuda humanitaria a Ucrania.

7. Conclusiones

Tanto en Europa como en España el futuro desarrollo de las TIC es prometedor, aprovechando las sinergias entre el mundo civil y el de seguridad y defensa. Tanto a nivel Comisión como de los países a nivel individual se ha tomado conciencia de la importancia que tienen estas tecnologías para nuestra autonomía estratégica. Se trata de un conjunto de tecnologías muy amplio y con posibilidades de cubrir necesidades de forma transversal para todas las capacidades militares. El gran reto es, quizás, integrar en los procesos de adquisición de sistemas las posibilidades de estas tecnologías de una forma flexible y ágil.

El impulso del sector civil y de las capacidades de las empresas, tanto de grandes multinacionales con importante presencia y actividad en España, como de empresas de diferente tamaño propiamente nacionales, permiten aventurar que las necesidades de defensa cuentan con el soporte necesario. Como ocurre en otros ámbitos, pero en este caso con mayor relevancia, la coordinación y la cooperación público-privada son aspectos necesarios para proporcionar un mejor servicio a los usuarios.

Las empresas asociadas en Aesmide cuentan con un conjunto de capacidades muy amplio para satisfacer las necesidades de información y comunicaciones en los ámbitos de seguridad y defensa en el entorno complejo en el que nos encontramos.

Enlaces

Análisis de Tecnologías Emergentes y Tendencias para el Soporte de Servicio de Combate del Ministerio de Defensa de Australia. **https://www.dst.defence.gov.au/sites/default/files/publications/documents/DST-Group-GD-0946.pdf**

Arquitectura Global de Sistemas y Tecnologías de Información y Comunicaciones del Ministerio de Defensa (AG CIS/TIC). 2017. **https://publicaciones.defensa.gob.es/arquitectura-global-de-sistemas-y-tecnologias-de-informacion-y-comunicaciones-del-ministerio-de-defensa-ag-cis-tic.html**

Campo de Batalla del Futuro. National Intelligence Council. The Future of Battlefield (2021). **https://www.dni.gov/files/images/globalTrends/GT2040/NIC-2021-02493--Future-of-the-Battlefield--Unsourced--14May21.pdf**

Estrategia de Comunicaciones Móviles de Quinta Generación (Estrategia 5G) del Ministerio de Defensa **https://publicaciones.defensa.gob.es/media/downloadable/files/links/b/o/bod_20210528_1_al.pdf**

Estrategia de Explotación de la Nube en el Ministerio de Defensa. **https://publicaciones.defensa.gob.es/media/downloadable/files/links/b/o/bod_20210528_1_al.pdf**

Estrategia de Modernización Digital US Department of Defence. Digital Modernization Strategy (2019). **https://media.defense.gov/2019/Jul/12/2002156622/-1/-1/1/DOD-DIGITAL-MODERNIZATION-STRATEGY-2019.PDF**

Estrategia de Tecnología e Innovación para la Defensa ETID-2020. **https://publicaciones.defensa.gob.es/estrategia-de-tecnologia-e-innovacion-para-la-defensa-etid-2020-libros-pdf.html**

European Industrial Srategy | European Commission (europa.eu). **https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-industrial-strategy_en**

Fondo Europeo de Defensa. **https://defence-industry-space.ec.europa.eu/eu-defence-industry/european-defence-fund-edf_en**

Hoja de Ruta Sobre Tecnologías Críticas para la Seguridad y la Defensa. **https://ec.europa.eu/info/files/communication-roadmap-critical-technologies-security-and-defence_en**

Internet de las Cosas Militares/en el Campo de Batalla. **https://www.computer.org/publications/tech-news/research/internet-of-military-battlefield-things-iomt-iobt**

Nube de Combate Multidominio. Saur, H. Multi-Domain Combat Cloud. Joint Air & Space Power Conference 2021. **https://www.japcc.org/essays/multi-domain-combat-cloud/**

Plan Estratégico de los Sistemas y Tecnologías de la Información y las Comunicaciones. 2018. **https://publicaciones.defensa.gob.es/plan-estrategico-de-los-sistemas-y-tecnologias-de-la-informacion-y-las-comunicaciones-del-ministerio-de-defensa-pecis.html**

Plan de Acción del Ministerio de Defensa para la Transformación Digital. 2020. **https://publicaciones.defensa.gob.es/plan-de-accion-del-ministerio-de-defensa-para-la-transformacion-digital-libro-pdf.html**

Plan de Acción sobre Sinergias entre Industrias Civiles, Defensa y Espacio Aprobado en 2021. **https://ec.europa.eu/info/files/action-plan-synergies-between-civil-defence-and-space-industries_en**

Tecnologías Críticas y Emergentes. National Science and Technology Council. Critical and emerging technologies list update (2022). Office of Science and Technologie Policy (OSTP). **https://www.whitehouse.gov/wp-content/uploads/2022/02/02-2022-Critical-and-Emerging-Technologies-List-Update.pdf**

Tecnologías de Computación Fronteriza (Edge Computing). National Defence Magazine. Viewpoint: The Rise of Edge Computing in Defense (2021). **https://www.nationaldefensemagazine.org/articles/2021/10/7/the-rise-of-edge-computing-in-defense**

Tecnologías Militares Emergentes. Sayler, K. M. (2022). Emerging Military Technologies. Congressional Research Service. **https://sgp.fas.org/crs/natsec/R46458.pdf**

Tendencias 2020-2040 de la Organización de Ciencia y Tecnología de la OTAN (STO). **https://www.nato.int/nato_static_fl2014/assets/pdf/2020/4/pdf/190422-ST_Tech_Trends_Report_2020-2040.pdf**

Siglas

AESMIDE. Asociación de Empresas Contratistas con las Administraciones Públicas.

BACSI. Base Aérea Conectada, Sostenible e Inteligente.

BLET. Base Logística del Ejército de Tierra.

CC. Combat Cloud – Nube de Combate.

CESTIC. Centro de Sistemas y Tecnologías de la Información y las Telecomunicaciones.

CIS. Communications and Information Systems – Sistemas de Información y Comunicación

COCS. Centro de Operaciones de Ciberseguridad.

DGAM. Dirección General de Armamento y Material.

EDA. European Defence Agency – Agencia Europea de Defensa.

EDAP. European Defence Action Plan – Plan de Acción Europeo de la Defensa.

EDF. European Defence Fund – Fondo Europeo de Defensa

EDIDP. European Defence Industrial Development Program – Programa Europeo de Desarrollo de la Industria de Defensa.

ETID. Estrategia de Tecnología e Innovación de la Defensa.

FCAS. Future Combat Air System – Futuro Sistema Aéreo de Combate.

IA. Inteligencia Artificial.

IoBT. Internet of Battlefield Things – Internet de las Cosas en el Campo de Batalla.

IoMT. Internet of Military Things – Internet de las Cosas Militar.

IoT. Internet of Things – Internet de las Cosas.

ISTAR. Intelligence, Surveillance, Target Acquisition and Reconnaissance – Inteligencia, Vigilancia, Adquisición de Objetivos y Reconocimiento.

I2D2. Inteligente, Interconectado, Distribuido y Digital.

I3D. Infraestructura Integral de Información de Defensa.

MDCC. Multi Domain Combat Cloud – Nube de Combate Multidominio.

PECIS. Plan Estratégico de los Sistemas y Tecnologías de la Información y las Comunicaciones.

PESCO. Permanent Structured Cooperation – Cooperación Estructurada Permanente.

SDN. Software Defined Networks – Redes Definidas por Software.

SDR. Software Defined Radio – Radio Definida por Software.

STO. Science and Technology Organization – Organización de Ciencia y Tecnología de la OTAN.

TIC. Tecnologías de la Información y las Comunicaciones.

OTAN. Organizacion del Tratado del Atlántico Norte.

UE. Unión Europea.

UME. Unidad Militar de Emergencias.

Edita

C/ Guzmán el Bueno, 98
28003 Madrid (España)
Telf.: +34 91 5940734
ids@idsolutions.biz
www.idsolutions.biz

Informe patrocinado por

aesmide
Asociación de Empresas Contratistas con las **Administraciones Públicas**
www.aesmide.es

GOBIERNO DE ESPAÑA · MINISTERIO DE INDUSTRIA, COMERCIO Y TURISMO · ICEX · UNIÓN EUROPEA