

Compendio sobre tecnologías facilitadoras y seguridad internacional

Edición de 2023

Sobre la autora



Wenting He es investigadora adjunta del Programa de Seguridad y Tecnología del UNIDIR. Posee un máster en Asuntos Internacionales por el Instituto Universitario de Altos Estudios Internacionales y del Desarrollo de Ginebra y una licenciatura en Diplomacia por la Universidad de Asuntos Exteriores de China, en Beijing.

Sobre el UNIDIR

El Instituto de las Naciones Unidas de Investigación sobre el Desarme (UNIDIR) es un instituto autónomo de las Naciones Unidas financiado con contribuciones voluntarias. UNIDIR, uno de los pocos institutos de políticas del mundo dedicado al desarme, genera conocimientos y promueve el diálogo y medidas en materia de desarme y seguridad. Tiene su sede en Ginebra, y ayuda a la comunidad internacional a desarrollar las ideas prácticas e innovadoras necesarias para hallar soluciones a problemas críticos para la seguridad.

Nota

Las denominaciones empleadas en esta publicación y la forma en que aparecen presentados los datos que contiene no implican, de parte de la Secretaría de las Naciones Unidas, juicio alguno sobre la condición jurídica de países, territorios, ciudades o zonas, o de sus autoridades, ni respecto de la delimitación de sus fronteras o límites. Las opiniones expresadas en la presente publicación son responsabilidad exclusiva de su autora. No reflejan necesariamente las opiniones de las Naciones Unidas, de UNIDIR o de la Unión Europea, así como tampoco de sus funcionarios o patrocinadores.

Agradecimientos

El apoyo de los patrocinadores principales del UNIDIR proporciona los cimientos de todas las actividades del Instituto. Esta publicación ha sido financiada por la Unión Europea en el marco del Programa de Seguridad y Tecnología del UNIDIR, que también cuenta con el apoyo de los Gobiernos de Alemania, la República Checa, Italia, Noruega, los Países Bajos y Suiza, así como de Microsoft.

La autora desea expresar su sincero agradecimiento al Dr. Giacomo Persi Paoli por su inestimable orientación y sus esclarecedoras aportaciones a lo largo de todo el proceso de redacción. Asimismo, desea agradecer en particular a Elia Duran-Smith su ayuda en la investigación exploratoria. Además, la autora da las gracias a James Black y Sarah Grand-Clément por su minuciosa revisión y sus constructivos comentarios, que han enriquecido enormemente el trabajo final.

Citación

He, Wenting. "Compendio sobre Tecnologías facilitadoras y seguridad internacional (edición de 2023)". Ginebra, Suiza: UNIDIR, 2024.

Abreviaturas y acrónimos

5G	Redes móviles de quinta generación
6G	Redes móviles de sexta generación
AlaaS	Inteligencia artificial como servicio
AWS	Amazon Web Services
CICR	Comité Internacional de la Cruz Roja
CPU	Unidad central de procesamiento
CSP	Proveedor de servicios en la nube
DOD	Departamento de Defensa (Estados Unidos)
EUV	Ultravioleta extrema
GNSS	Sistema mundial de navegación por satélite
GPU	Unidad de procesamiento gráfico
IA	Inteligencia artificial
IaaS	Infraestructura como servicio
IoMT	Internet de las cosas militares
IoT	Internet de las cosas
ISR	Inteligencia, vigilancia y reconocimiento
JWCC	Joint Warfighting Cloud Capability
MRI	Imagen por resonancia magnética
NEMS	Sistemas nanoelectromecánicos
nm	Nanómetro
NPU	Unidades de procesamiento neuronal
OTB	Órbita terrestre baja
PaaS	Plataforma como servicio
PQC	Criptografía poscuántica
QKD	Distribución cuántica de claves
RA	Realidad aumentada
RV	Realidad virtual
SaaS	Software como servicio
SAT	Superconductores de alta temperatura
SoC	Sistema en un chip
TIC	Tecnología de la información y las comunicaciones

TPU	Unidad de procesamiento tensorial
TSMC	Taiwan Semiconductor Manufacturing Company
UAV	Vehículo aéreo no tripulado

Índice

Sobre la autora	1
Sobre el UNIDIR	1
Nota	1
Agradecimientos	2
Citación.....	2
Abreviaturas y acrónimos.....	3
Resumen.....	5
1. Introducción	6
2. Categoría I: materiales avanzados.....	7
2.1 Semiconductores.....	7
2.2 Superconductores	10
2.3 Nanotecnología	11
3. Categoría II: Piezas y componentes	13
3.1 Microchips.....	13
3.2 Sensores.....	16
4. Categoría III: Procesamiento y computación	18
4.1 Computación en la nube	18
4.2 Computación perimetral	20
4.3 Computación cuántica.....	22
5. Categoría IV: Infraestructura	25
5.1 5G y 6G	25
5.2 Internet de las cosas	27
5.3 Infraestructura en la nube	28
5.4 Comunicaciones por satélite.....	30

6. Conclusión.....	32
Referencias.....	35

Resumen

El desarrollo tecnológico en ámbitos como los materiales avanzados, los microchips, los sensores y la infraestructura de conectividad permite innovaciones en otras áreas tecnológicas, en particular, las tecnologías de la información y las comunicaciones (TIC), la inteligencia artificial (IA) y los sistemas autónomos. Estas tecnologías facilitadoras están transformando el panorama digital y poseen potencial de aplicación en el ámbito militar. Aunque se ha avanzado en el abordaje de las consecuencias de las TIC y la IA para la seguridad en el marco de diversos procesos intergubernamentales, en términos relativos se ha prestado menos atención a las tecnologías subyacentes que facilitan o impulsan su desarrollo ulterior. Ello pone de relieve la urgente necesidad de un examen más profundo y exhaustivo de las tecnologías facilitadoras, así como de sus posibles repercusiones en la seguridad internacional.

Para colmar esta laguna de conocimientos, este compendio se dedica a la identificación y el análisis de los avances más destacados en tecnologías facilitadoras, con especial atención a aquellas que aún se encuentran en sus primeras fases de desarrollo o aplicación. Este compendio explora cuatro categorías de tecnologías facilitadoras: materiales avanzados (semiconductores, superconductores y nanotecnología), piezas y componentes (microchips y sensores), procesamiento y computación (computación en la nube, perimetral (del inglés *Edge*) y cuántica) e infraestructura (telecomunicaciones de quinta y sexta generación [5G y 6G], Internet de las cosas, infraestructura en la nube y comunicaciones por satélite).

Este compendio destaca varias tendencias y avances generales en los ámbitos tecnológicos analizados. La actual tendencia a la miniaturización del *hardware* conduce a la creación de dispositivos cada vez más pequeños y eficientes, lo que facilita la integración generalizada de las tecnologías facilitadoras en los sistemas militares. Estas tecnologías ofrecen mejoras significativas en las capacidades militares y el potencial para reforzar los esfuerzos de seguridad internacional. Sin embargo, surgen retos derivados del posible aumento de la competencia tecnológica entre Estados y de los riesgos y vulnerabilidades de ciberseguridad en la cadena de suministro mundial que están asociados a las tecnologías facilitadoras. Aunque el sector privado desempeña un papel fundamental, la colaboración en tecnologías de doble uso puede plantear nuevos riesgos, poniendo, por ejemplo, en peligro la información militar sensible.

El seguimiento y el análisis continuos de las tendencias emergentes son, por tanto, esenciales para establecer marcos de gobernanza efectivos que equilibren las oportunidades y los riesgos que plantean las tecnologías facilitadoras.

1. Introducción

Tecnologías como los materiales avanzados, los microchips y los sensores, la potencia de computación y la infraestructura de conectividad permiten o impulsan la innovación y el desarrollo de capacidades en otros ámbitos tecnológicos, especialmente las TIC, la IA y los sistemas autónomos. Los avances de las tecnologías facilitadoras están revolucionando el ecosistema digital, ampliando sus posibilidades de desarrollo y aplicación con fines militares¹. Con el desarrollo de estas tecnologías se hace cada vez más importante abordar sus consecuencias para la paz y la seguridad internacionales. Para aprovechar las ventajas de estas tecnologías y mitigar al mismo tiempo sus posibles riesgos, es esencial una continua exploración de horizontes.

En el informe 2023 sobre “Los avances científicos y tecnológicos actuales y sus posibles efectos en las iniciativas relacionadas con la seguridad internacional y el desarme”, el Secretario General de las Naciones Unidas subraya la continua preocupación por el hecho de que los avances científicos y tecnológicos de importancia para la seguridad y el desarme estén superando la capacidad de los marcos normativos y de gobernanza para gestionar los riesgos². Aunque varios procesos intergubernamentales han avanzado notablemente en el abordaje de las consecuencias de las TIC y la IA para la seguridad, en términos relativos, se ha prestado menos atención a las tecnologías subyacentes que permiten o impulsan su desarrollo. Ello pone de relieve la urgente necesidad de un examen más profundo y exhaustivo de las tecnologías facilitadoras, así como de sus posibles repercusiones en la seguridad internacional.

En un esfuerzo por colmar esta laguna de conocimientos, el presente compendio está dedicado a la identificación y el análisis de los avances más notorios de las tecnologías facilitadoras. Se incluyen aquellas que aún se encuentran en las primeras fases de su desarrollo o aplicación, pero que previsiblemente tendrán repercusiones importantes en la paz y la seguridad internacionales. Este compendio se centra exclusivamente en el análisis de los efectos de primer orden de las tecnologías facilitadoras en el ecosistema digital, específicamente aquellos relevantes para la paz y la seguridad internacionales. Sin embargo, algunas áreas tecnológicas pueden tener implicaciones de mayor alcance que las abordadas en el presente informe.

En los capítulos siguientes, el compendio profundiza en cuatro categorías de tecnologías facilitadoras. La categoría I se refiere a los materiales avanzados, como los semiconductores, los superconductores y la nanotecnología. La categoría II se ocupa de las piezas y los componentes, incluidos los microchips y los sensores. La categoría III abarca el procesamiento y la computación, es decir, la computación en la nube, la computación perimetral y computación cuántica. La categoría IV corresponde a las infraestructuras, desde las telecomunicaciones de quinta y sexta generación (5G y 6G), pasando por de Internet de las cosas (IoT) y la infraestructura en la nube, hasta las comunicaciones por satélite. Cada capítulo presenta un análisis exhaustivo de la

¹ A efectos de este compendio, las tecnologías facilitadoras se definen como aquellas que permiten o impulsan la innovación y el desarrollo de capacidades en otros campos tecnológicos contemplados dentro del ámbito de trabajo del Programa de Seguridad y Tecnología del UNIDIR: cibernética, IA y autonomía e integración de sistemas.

² AGNU (2023).

tecnología examinada, incluidos los últimos avances y las aplicaciones militares pertinentes, seguido de una evaluación de las posibles consecuencias para la seguridad internacional. El compendio concluye con un examen global de las tendencias generales y la evolución en el ámbito de las tecnologías facilitadoras.

2. Categoría I: materiales avanzados

2.1 Semiconductores

Los semiconductores pertenecen a una clase de materiales que se caracterizan por poseer propiedades de conductividad eléctrica que se sitúan entre las de los conductores (por ejemplo, los metales) y los aislantes (como el vidrio). La conductividad eléctrica de un semiconductor puede controlarse y modificarse, lo que permite utilizarlo como componente básico de dispositivos y componentes electrónicos modernos, como diodos, transistores y circuitos integrados.

Las propiedades eléctricas únicas de los semiconductores han transformado el panorama tecnológico, dando lugar al desarrollo de dispositivos y sistemas electrónicos cada vez más pequeños, potentes y energéticamente eficientes. En la industria electrónica, el silicio es el material semiconductor por excelencia, pero también se emplean otros como el arseniuro de galio y el germanio en aplicaciones especializadas. Las obleas de silicio suelen servir de base para la fabricación de microchips y desempeñan un papel esencial en el funcionamiento de las tecnologías digitales.

El nodo de proceso de los semiconductores, que ahora suele medirse en nanómetros (nm)³, es un factor crítico en esta tecnología. El menor tamaño de los nodos de proceso permite introducir más transistores en un solo chip, lo que suele mejorar el rendimiento y la eficiencia energética. Las dimensiones de los nodos de los semiconductores se han reducido considerablemente a lo largo de las décadas; inicialmente se medían en micrómetros (μm)⁴ y, hoy en día, los más avanzados tecnológicamente son de 3 nm⁵. Taiwan Semiconductor Manufacturing Company (TSMC), uno de los fabricantes de semiconductores más avanzados, tiene previsto producir la próxima generación de semiconductores de 2 nm a partir de 2025. Con ello se prevé alcanzar velocidades de procesamiento entre un 10 % y un 15 % superiores a las de los chips de 3 nm.⁶

³ Un nanómetro equivale a la milésima parte de un micrómetro, o a la milmillonésima parte de un metro.

⁴ Por ejemplo, el procesador 4004 de Intel lanzado en 1971:

<https://www.intel.com/content/www/us/en/history/museum-story-of-intel-4004.html>

⁵ En septiembre de 2023, solo dos empresas del mundo podían fabricar semiconductores de 3 nm:

TSMC(https://www.tsmc.com/english/dedicatedFoundry/technology/logic/l_3nm)y

Samsung(<https://news.samsung.com/global/samsung-begins-chip-production-using-3nm-process-technology-with-gaa-architecture>).

⁶ Ryugen, Hideaki (2023).

La fuerza motriz de la evolución de los nodos de proceso es lo que se conoce como Ley de Moore. Se trata de una observación empírica de Gordon Moore, uno de los cofundadores de Intel, según la cual, a lo largo de su historia el número de transistores de un microchip ha tendido a duplicarse aproximadamente cada dos años. Por tanto, la ley afirma que el rendimiento computacional seguirá aumentando mientras disminuya el coste de los ordenadores. Aunque la teoría se ha mantenido en gran medida incontestada en el siglo XXI, los ingenieros han empezado a alcanzar los límites de los materiales semiconductores tradicionales según la comprensión actual de las leyes de la física. Por ello, algunos observadores incluso sostienen que la Ley de Moore ha quedado obsoleta⁷. La industria busca ahora soluciones innovadoras para seguir mejorando los semiconductores en el futuro.

En lugar del silicio, se han identificado otros materiales como posibles alternativas para satisfacer la creciente demanda de potencia de computación. En los semiconductores compuestos, por ejemplo, se combinan múltiples elementos para crear materiales que ofrecen mejores prestaciones que el silicio. Estos materiales están llamados a desempeñar un papel fundamental en la evolución de las nuevas tecnologías de conectividad y los vehículos autónomos⁸. El arseniuro de galio, el segundo material semiconductor más utilizado después del silicio, es un compuesto conocido por presentar una mayor movilidad de electrones que le confiere una eficiencia superior a la del silicio. También presenta una mayor tolerancia al sobrecalentamiento. Sin embargo, la producción a gran escala de arseniuro de galio debe aún superar importantes desafíos, como la dependencia de sustancias químicas tóxicas que suscitan inquietud por sus consecuencias para la salud pública y el medio ambiente⁹.

Se están investigando nuevos materiales con un gran potencial para facilitar el desarrollo de dispositivos cada vez más pequeños y eficientes. Estudios recientes han puesto de relieve la eficacia de un material llamado arseniuro de boro cúbico, que podría solventar ciertas limitaciones que presentan los semiconductores tradicionales de silicio y convertirse en el "mejor material semiconductor hallado hasta la fecha"¹⁰. A pesar de sus prometedoras propiedades, el arseniuro de boro cúbico se encuentra actualmente en fase experimental, por lo que sus aplicaciones en el mundo real aún están por determinar. Paralelamente, también están ganando terreno otros materiales semiconductores emergentes, como el nitruro de galio de alta potencia, los materiales basados en el antimoniuro y el bismuturo, y los materiales bidimensionales (2D) como el grafeno¹¹. Estos materiales presentan propiedades físicas características que aportan un valor añadido para aplicaciones específicas. Sin embargo, su uso generalizado se ve limitado por los costes y la complejidad de su producción.

La continua innovación en materiales semiconductores desempeñará un papel fundamental en los futuros sistemas militares. Los semiconductores tienen aplicaciones concretas en toda una serie de componentes críticos de los dispositivos electrónicos, como los sensores, los actuadores

⁷ Arcuri and Shivakumar (2022).

⁸ IEEE (n.d.-a).

⁹ IEEE (n.d.-b).

¹⁰ Chandler (2022).

¹¹ IEEE (n.d.-b).

y los chips de memoria o los sistemas electroópticos y los microcontroladores ¹². Estos semiconductores son componentes esenciales de dispositivos electrónicos de última generación de gran importancia para sofisticados sistemas militares, como los dispositivos de comunicaciones de alta velocidad, los sistemas de radar y el armamento guiado de precisión. Además, la tecnología de semiconductores sirve de catalizador para innovaciones transformadoras como la inteligencia artificial o Internet de las cosas (IoT). Así pues, la aparición de nuevos materiales semiconductores podría reforzar las capacidades nacionales de defensa, aunque también podría marcar el comienzo de una nueva era de competencia tecnológica entre los Estados.

Por otra parte, las vulnerabilidades de la cadena de suministro representan actualmente un reto de vital importancia. La cadena de suministro de los semiconductores es una red mundial muy compleja e interconectada en la que intervienen varias fases de producción y empresas de distintas regiones. También se caracteriza por un alto grado de especialización, como demuestra, por ejemplo, la concentración de instalaciones de producción de semiconductores avanzados en Asia Oriental. Cualquier alteración en las capacidades de fabricación en la región, ya sea derivada de tensiones geopolíticas o de catástrofes naturales, podría repercutir negativamente en la disponibilidad de semiconductores y tener graves consecuencias para la seguridad nacional. Sin embargo, el desarrollo de materiales semiconductores alternativos podría transformar el

Semiconductores: lo más destacado de 2023

- Se están produciendo continuos avances en la creación de semiconductores más pequeños y eficientes. Los principales fabricantes de semiconductores, como [TSMC](#) y [Samsung](#), se consagran al desarrollo de la próxima generación de tecnología de semiconductores de 2 nm, la cual, según las proyecciones, aumentará la velocidad de procesamiento entre un 10 % y un 15 % respecto a los semiconductores de 3 nm más avanzados existentes en la actualidad.
- El silicio sigue siendo el material semiconductor más utilizado, pero se está acercando a sus límites físicos. Las investigaciones en curso exploran nuevos materiales semiconductores con potencial para mejorar el rendimiento, entre ellos el [arseniuro de boro cúbico](#) y [los materiales 2D](#).
- La cadena de suministro de semiconductores es vulnerable a las alteraciones derivadas de su naturaleza compleja e interconectada, lo que puede suponer un grave problema para la seguridad nacional. No obstante, la exploración de materiales semiconductores alternativos podría contribuir a diversificar la cadena de suministro mundial.

paradigma actual y aumentar la diversificación dentro de la cadena de suministro mundial.

¹² Gargeyas (2022).

2.2 Superconductores

Los superconductores son materiales capaces de conducir la electricidad sin resistencia ni pérdida de energía y de repeler los campos magnéticos cuando se enfrían por debajo de una temperatura crítica específica. Esta propiedad única permite que una corriente eléctrica fluya indefinidamente dentro de un superconductor.

Las excepcionales características electromagnéticas de los superconductores pueden aportar mejoras en diversos campos, como la electrónica, la computación cuántica, la transmisión y el almacenamiento de energía o la tecnología de imagen por resonancia magnética (MRI). Sin embargo, su uso práctico se ve limitado actualmente por el requisito de temperaturas extremadamente bajas que implican una costosa ingeniería criogénica y un elevado consumo de energía en el proceso de enfriamiento. La mayoría de los materiales superconductores presentan temperaturas críticas que oscilan entre el cero absoluto y 10 Kelvin (aproximadamente entre -273 y -263 grados Celsius)¹³. Por consiguiente, la aplicación a gran escala de los superconductores resulta actualmente impracticable.

La investigación en materia de superconductividad se ha centrado principalmente en la búsqueda de materiales con temperaturas críticas mucho más elevadas. Se han descubierto superconductores de alta temperatura (SAT) que presentan superconductividad a temperaturas más altas que los materiales convencionales. A pesar de denominarse “de alta temperatura”, los SAT son materiales que conducen la electricidad por encima de 77 Kelvin (-196,2 grados Celsius), que es el punto de ebullición del nitrógeno líquido¹⁴. En los últimos años, la comunidad científica ha redoblado sus esfuerzos por ampliar los límites de la superconductividad hasta llegar a la temperatura ambiente. Se trata de una investigación en curso, pero hasta ahora no se ha logrado ningún avance significativo.

Los futuros esfuerzos de investigación y desarrollo pueden reducir eficazmente los costes operativos y hacer que la tecnología de superconductividad sea más accesible para las aplicaciones prácticas. Se prevé que el uso de superconductores avanzados en contextos militares ejerza un efecto transformador. El desarrollo de materiales superconductores escalables a temperatura ambiente podría revolucionar el campo de la electrónica y dar lugar a aplicaciones tan prometedoras como microchips de velocidad ultrarrápida y bajo consumo energético, comunicaciones inalámbricas de banda ancha y baja latencia y redes eléctricas de alta eficiencia¹⁵. Los superconductores pueden utilizarse asimismo para construir cúbits (las unidades básicas de los procesadores cuánticos), con las enormes oportunidades que ello supondría para la computación cuántica¹⁶. Se están desarrollando nuevos materiales superconductores para

¹³ NCCR (National Centre of Competence in Research, 2021). La temperatura crítica es la temperatura a la que la resistencia eléctrica de un superconductor desciende hasta cero.

¹⁴ Clynes (2023).

¹⁵ Pedram (2023).

¹⁶ Véase en el apartado 4.3 un análisis detallado sobre la computación cuántica y sus últimos avances.

generar cúbits resistentes a perturbaciones externas, una característica que ampliaría notablemente la fiabilidad de los ordenadores cuánticos¹⁷. Sin embargo, la aparición de los superconductores a temperatura ambiente podría alentar un nuevo campo de competencia tecnológica entre Estados y desencadenar disputas internacionales en torno a cuestiones como las patentes, la transferencia de tecnología o el acceso a los mercados¹⁸.

Superconductores: lo más destacado de 2023

- En la actualidad, la aplicación práctica de los superconductores se ve condicionada por la necesidad de temperaturas extremadamente bajas, que exigen una costosa ingeniería criogénica y un elevado consumo energético. Los esfuerzos de la comunidad científica se consagran al desarrollo de superconductores a temperatura ambiente.
- El desarrollo de superconductores escalables a temperatura ambiente promete revolucionar el campo de la electrónica, pero su aparición podría suscitar disputas internacionales en torno a cuestiones como las patentes, la transferencia de tecnología y el acceso a los mercados.

2.3 Nanotecnología

La nanotecnología contribuye al diseño, la fabricación y la aplicación de materiales a escala nanométrica, normalmente de entre 1 y 100 nanómetros (un nanómetro es la milmillonésima parte de un metro).

A escala nanométrica surgen propiedades únicas y a menudo novedosas como resultado de los efectos cuánticos y el comportamiento de las superficies¹⁹. Estas propiedades pueden aprovecharse para diversas aplicaciones, como los nanomateriales y la nanoelectrónica. En la electrónica moderna, los avances en los sistemas nanoelectromecánicos (NEMS) están facilitando considerablemente la actual tendencia a la miniaturización de los dispositivos. Estos sistemas pueden utilizarse para fabricar sensores, actuadores y otros dispositivos más pequeños y eficientes con aplicaciones críticas en los campos de la detección avanzada, la informática y las comunicaciones.

En las aplicaciones de detección, la nanotecnología se aplica al control medioambiental de la calidad del aire y del agua, así como a la detección de contaminantes. La incorporación de la nanotecnología permite fabricar sensores más pequeños y sensibles para operaciones militares sobre el terreno capaces, por ejemplo, de detectar agentes que constituyan amenazas biológicas y químicas. En comparación con los métodos convencionales de detección de amenazas

¹⁷ Feldman (2023).

¹⁸ Roa (2023).

¹⁹ US National Nanotechnology Coordination Office (n.d.).

biológicas, los biosensores basados en nanomateriales ofrecen una mayor sensibilidad y precisión incluso con un volumen de muestra, un tiempo de preparación y unos costes de ensayo reducidos²⁰. Los nanosensores pueden proporcionar información en tiempo real sobre posibles amenazas para las operaciones militares, mejorando así la conciencia situacional en el campo de batalla. Asimismo, pueden contribuir a los esfuerzos de verificación del desarme en los ámbitos de las armas biológicas y químicas.

En el campo de la informática, la nanotecnología sienta las bases de la computación de última generación al facilitar el desarrollo de nanomateriales como los nanotubos de carbono, el grafeno y los puntos cuánticos. Habida cuenta de que la tecnología convencional basada en el silicio se acerca a sus límites físicos, crece el interés por materiales y enfoques alternativos para nuevos paradigmas informáticos. En los últimos años, los investigadores plantean que los nanotubos de carbono pueden ser una alternativa atractiva para sustituir al silicio en la fabricación de transistores²¹. El uso de este nanomaterial altamente conductor puede facilitar la creación de transistores más compactos y eficientes con prestaciones superiores a las de los basados en el silicio²². Sin embargo, aún no se han demostrado de forma concluyente sus ventajas en aplicaciones reales²³. Por otra parte, los puntos cuánticos (es decir, los nanocristales sintetizados mediante el proceso de nanofabricación) pueden revolucionar el campo de la computación cuántica. Gracias a sus propiedades cuánticas, los puntos cuánticos pueden utilizarse como cúbits —la base misma de los ordenadores cuánticos—, para crear la estructura de una máquina de trabajo escalable, rentable y tolerante a fallos.²⁴ Sin embargo, esta tecnología sigue en pañales y se enfrenta a varias dificultades técnicas y comerciales que deben superarse para hacer posible la producción viable y a gran escala de ordenadores cuánticos²⁵.

Además, la nanotecnología puede facilitar las comunicaciones avanzadas en operaciones militares gracias a sus múltiples ventajas, como un menor consumo de energía, una conectividad mejorada o la posibilidad de crear dispositivos de comunicación miniaturizados. En el ámbito de los sistemas de comunicaciones inalámbricas, los avances de la nanotecnología dan lugar al desarrollo de dispositivos sensores inalámbricos más pequeños, eficientes y económicos que consumen menos energía y hacen posibles las redes 5G²⁶. Los nanomateriales también pueden utilizarse para crear antenas de alta eficiencia capaces de mejorar el rendimiento y la fiabilidad de la señal. Por ejemplo, los investigadores han desarrollado nanoantenas que permiten la transferencia de datos a la velocidad de la luz entre distintos núcleos de procesadores sin apenas pérdidas²⁷.

Aunque la nanotecnología alberga un gran potencial de mejora de los sistemas militares de información y comunicaciones, su desarrollo y despliegue también entrañan ciertos riesgos.

²⁰ Rowland et al. (2016).

²¹ Fadelli (2023).

²² Basheer et al. (2022).

²³ Fadelli (2023).

²⁴ Hecht (2022).

²⁵ Véase en el apartado 4.3 un análisis detallado sobre la computación cuántica y sus últimos avances.

²⁶ Hamza and Jaafar (2022).

²⁷ Kullock et al. (2020).

Según los estudios, las nanopartículas pueden comportar riesgos medioambientales y de toxicidad de muy diversa índole que supondrían un grave riesgo tanto para la salud humana como para el bienestar ecológico.²⁸ Por su tamaño y composición, las nanopartículas pueden traspasar las barreras fisiológicas de los organismos vivos y provocar reacciones biológicas nocivas dentro del cuerpo humano (tales como inflamación pulmonar o problemas cardíacos)²⁹. Los nanomateriales resultantes de procesos de fabricación pueden acceder al medio ambiente a través de emisiones tanto deliberadas como accidentales. Una vez depositados en el suelo, podrían contaminar el terreno y filtrarse posteriormente a los sistemas hídricos³⁰.

Nanotecnología: lo más destacado de 2023

- Los continuos avances en nanotecnología mejoran constantemente las tecnologías avanzadas de detección, computación y comunicaciones. Algunos nanomateriales, como los nanotubos de carbono y los puntos cuánticos, poseen potencial para impulsar la computación de nueva generación, incluido el campo emergente de la computación cuántica. Sin embargo, persisten los problemas para lograr una producción viable y a gran escala.
- La nanotecnología ofrece ventajas para los sistemas de información y comunicaciones militares, pero también presenta riesgos. Las investigaciones indican que las nanopartículas pueden ser tóxicas y peligrosas para el medio ambiente y plantear importantes riesgos para la salud humana y el bienestar ecológico.

3. Categoría II: Piezas y componentes

3.1 Microchips

Los microchips, también conocidos como chips o circuitos integrados, son conjuntos compactos de componentes electrónicos miniaturizados que constan de transistores, diodos y resistencias instalados en una pequeña pieza plana de material semiconductor, normalmente una oblea de silicio.

Nunca se insistirá lo suficiente en la importancia de la tecnología de microchips. Constituye la piedra angular de la electrónica moderna y los sistemas informáticos y hace posible desarrollar dispositivos que no solo son más pequeños, sino también más potentes, rentables y energéticamente eficientes que los construidos con componentes discretos. Los microchips pueden desempeñar diversas funciones críticas, como el procesamiento de información, el almacenamiento de datos y la ejecución de instrucciones, y pueden utilizarse como chips de memoria, unidades centrales de procesamiento (CPU) y unidades de procesamiento gráfico (GPU).

²⁸ Kumah et al. (2023).

²⁹ Ibid.

³⁰ Ray, Paresh et al. (2009).

Los microchips evolucionan constantemente, gracias a los avances en los materiales semiconductores, que permiten nuevas funcionalidades y mayor rendimiento a menor coste³¹. Como ya se ha descrito, la industria de los semiconductores sigue ampliando los límites de la miniaturización, permitiendo el desarrollo de transistores con nodos de proceso más pequeños. La reducción del tamaño permite colocar más transistores en un mismo microchip, lo que se traduce en una mayor capacidad informática y eficiencia energética. Sin embargo, dado que la actual tecnología de semiconductores basada en el silicio se está acercando a sus límites físicos, se buscan materiales y enfoques alternativos para garantizar el desarrollo y la transformación continuos de la tecnología de microchips.

La innovación en este campo también se ve impulsada por la mejora en el diseño de los chips. Se han propuesto métodos alternativos de diseño de chips, como los "sistemas *multi-die*" y el diseño basado en chiplets³². A diferencia de los chips monolíticos tradicionales, la "arquitectura *multi-die*" consiste en un conjunto de chips especializados, como los de memoria y CPU, que pueden conectarse para crear un paquete complejo e integrado con tecnología SoC ("sistema en un chip", por sus siglas en inglés). Se cree que este innovador diseño de chip puede dar soporte al aprendizaje automático de IA a escala, mejorar la tasa de rendimiento del silicio y minimizar los residuos del proceso de fabricación de chips³³. Empresas como Apple, Google/Alphabet y Amazon Web Services (AWS) diseñan SoC personalizados para optimizar el rendimiento de los chips en aplicaciones y cargas de trabajo específicas, lo que se conoce como enfoque de "silicio personalizado"³⁴.

Se están diseñando microchips especializados que facilitan otras aplicaciones tecnológicas como el 5G y la inteligencia artificial. La conectividad 5G requiere el desarrollo de microchips avanzados que puedan satisfacer los requisitos de alta velocidad y baja latencia de dicha tecnología. Las capacidades de la IA también dependen en gran medida de la capacidad informática de los microchips especializados, como las unidades de procesamiento tensorial (TPU) y las unidades de procesamiento neuronal (NPU). Los chips de IA de última generación pueden ser decenas o miles de veces más rápidos y eficientes que los chips genéricos, como las CPU³⁵.

Además, la tecnología de litografía ultravioleta extrema (EUV) desempeña actualmente un papel importante en la fabricación de los microchips más avanzados del mundo. Esta tecnología hace posible la creación de componentes ultrapequeños y muy precisos en obleas de silicio y contribuye a la continua miniaturización de los microchips. Para avanzar en el proceso de miniaturización, los investigadores han identificado un método más complejo, conocido como litografía EUV de alta apertura numérica, para poder producir en masa la próxima generación de tecnología de nodos de 2 nm³⁶. Se espera que los nuevos sistemas de fabricación estén plenamente operativos en 2025³⁷. Además, los métodos avanzados de empaquetado también

³¹ Véase en el apartado 2.1 un análisis detallado de la tecnología de semiconductores y sus últimos avances.

³² MIT Technology Review Insights (2023).

³³ Ibid.

³⁴ Shilov (2023).

³⁵ Khan and Mann (2020).

³⁶ IBM (2023).

³⁷ ASML (n.d.).

aportan mejoras en el rendimiento y la eficiencia energética de los microchips, sobre todo las técnicas de apilamiento y empaquetado tridimensional (3D) que integran varios chips en una estructura tridimensional³⁸.

Los nuevos avances en tecnología de microchips seguirán configurando el panorama tecnológico en los próximos años, lo que tendrá importantes implicaciones para la seguridad internacional. El papel omnipresente de los sistemas electrónicos en la guerra moderna significa que la mejora del rendimiento de los microchips puede aportar beneficios en diversos aspectos de las operaciones militares. Entre ellos se incluyen el aumento de la precisión y la eficacia del armamento avanzado, el aumento de las capacidades de inteligencia, vigilancia y reconocimiento (ISR), la mejora de los sistemas de comunicaciones y la facilitación de la integración de la IA y la autonomía en los sistemas militares. Sin embargo, la tecnología también plantea nuevos retos de seguridad. La cadena de suministro de microchips está muy globalizada y es muy compleja en sus distintas fases; desde el diseño y la fabricación de chips hasta el empaquetado, las pruebas y la distribución. Las tecnologías y las capacidades de fabricación más avanzadas suelen concentrarse en determinadas regiones, lo que crea posibles vulnerabilidades en la cadena de suministro. Por ejemplo, la empresa neerlandesa ASML es actualmente la única con capacidad para fabricar las máquinas de litografía EUV utilizadas para la producción a gran escala de los microchips más avanzados del mundo³⁹.

Otro aspecto problemático es el doble uso de la tecnología y su potencial de proliferación. Los microchips utilizados en aplicaciones civiles, como los teléfonos inteligentes y los ordenadores portátiles, pueden quedar fuera de la normativa de control de exportaciones y, por tanto, ser explotados con fines militares o integrados en sistemas militares⁴⁰. El uso de microchips también plantea problemas de ciberseguridad. Las vulnerabilidades del *hardware* son difíciles de detectar, dada la complejidad de la arquitectura de los circuitos integrados. Las modificaciones físicas pueden ocultarse eficazmente entre la gran variedad de componentes y funciones válidos y pasar desapercibidas durante mucho tiempo⁴¹. En comparación con los problemas de *software*, los fallos de *hardware* suelen ser bastante más difíciles y costosos de solucionar, lo que constituye una vulnerabilidad y pone en riesgo los sistemas digitales en general⁴².

³⁸ Moore (2022).

³⁹ ASML (n.d.).

⁴⁰ Gilchrist (2023).

⁴¹ Levine and Pipikaite (2019).

⁴² Giles (2019).

Microchips: lo más destacado de 2023

- Los avances en la tecnología de semiconductores siguen impulsando un mayor rendimiento y funcionalidad de los microchips a menor coste gracias a la miniaturización. La exploración de materiales y enfoques alternativos para el desarrollo de semiconductores posee potencial para apoyar el crecimiento y la transformación de la tecnología de microchips.
- Los avances en este campo también se deben a la mejora en el diseño de los chips y las técnicas de producción. Los innovadores diseños de chips, como los “sistemas multi-die”, ofrecen complejos sistemas de chips integrados y compatibles con el aprendizaje automático de IA a escala. Se está desarrollando la tecnología de litografía EUV de alta apertura numérica, cuyo objetivo es permitir la producción en masa de la próxima generación de tecnología de nodos de 2 nm para 2025.
- A pesar de los posibles beneficios que aporta la mejora del rendimiento de los microchips a las operaciones militares, también conlleva retos, como las vulnerabilidades de la cadena de suministro, la naturaleza de doble uso de la tecnología y los problemas de ciberseguridad.

3.2 Sensores

Los sensores son dispositivos diseñados para detectar propiedades físicas y condiciones ambientales y, posteriormente, convertir esta información en señales de salida.

Los sensores —que pueden ser de movimiento, de proximidad, biométricos o de imagen, entre otros— poseen gran variedad de aplicaciones y funcionalidades. Se han convertido en elementos indispensables en casi todas las facetas de los sistemas militares; desde vehículos terrestres, buques y vehículos aéreos no tripulados (UAV) hasta misiles y satélites. Así pues, los avances en la tecnología de sensores desempeñan un papel fundamental en la modernización de las capacidades de defensa y pueden aumentar la eficacia global de las operaciones militares. Las aplicaciones de sensores avanzados brindan a las fuerzas armadas la posibilidad de recopilar datos más precisos y adecuados, mejorar la conciencia situacional y la protección en el campo de batalla, mejorar la precisión de los objetivos y la detección de amenazas y facilitar la toma de decisiones en entornos operativos dinámicos.

Han surgido numerosos avances en el ámbito de la tecnología de sensores con fines militares. La fusión de datos de sensores representa un área clave de innovación. Las fuerzas armadas están cada vez más interesadas en combinar las lecturas de múltiples sensores para obtener información más precisa y completa sobre el campo de batalla. Los sistemas multisensor integran y analizan datos procedentes de diversos tipos de sensores (acústicos, de radar, electroópticos e infrarrojos), mejorando la conciencia situacional hasta un nivel superior al que puede alcanzarse normalmente analizando estas fuentes por separado. En los vehículos militares terrestres, la tecnología de fusión

de datos de sensores proporciona a la tripulación o al comandante una visión completa de 360 grados de su entorno y facilita el intercambio de información con otros sistemas⁴³.

La detección cuántica aprovecha la sensibilidad inherente de los estados cuánticos a las perturbaciones, lo que no solo permite realizar mediciones más precisas y sensibles, sino también medir fenómenos antes no mensurables.⁴⁴ La detección cuántica puede transformar las capacidades militares. Por ejemplo, los investigadores han desarrollado sensores cuánticos capaces de detectar objetos ocultos tras muros y otras barreras, que pueden resultar de utilidad en aplicaciones militares como las de reconocimiento⁴⁵. Asimismo, la tecnología de detección cuántica podría mejorar la precisión de los sistemas de navegación inercial utilizados en barcos, submarinos y aviones. Ello mejoraría significativamente las capacidades de posicionamiento y navegación en entornos sin señal GNSS⁴⁶.

Cada vez con más frecuencia, los sensores incorporan tecnologías de IA y permiten por tanto un análisis y recopilación inteligentes de los datos, lo cual redundaría en la eficacia de la toma de decisiones militares. Los sistemas de radar cognitivos emplean capacidades de aprendizaje automático para adaptarse a los cambios en el entorno o en el comportamiento de un adversario⁴⁷. Además, también se han desarrollado sensores biométricos ponibles para el seguimiento en tiempo real de las constantes vitales de los soldados (frecuencia cardíaca, temperatura corporal, hidratación, etc.), así como sus estados mentales, incluidos los niveles de cansancio y estrés. La integración de la IA en los futuros sistemas será fundamental para agilizar el filtrado e interpretación de los datos recogidos por los dispositivos ponibles que llevan los soldados⁴⁸. Este nuevo avance podría ayudar a los mandos a tomar decisiones militares y mejorar el rendimiento del personal militar.

Además de mejorar las capacidades militares, los avances en la tecnología de detección presentan nuevas oportunidades para la paz y la seguridad internacionales. La tecnología de teledetección puede asistir en la supervisión de los conflictos armados en curso y el cumplimiento de los acuerdos de paz⁴⁹. El uso de sensores avanzados también permite detectar más eficazmente sustancias peligrosas, como agentes químicos y biológicos, en el medio ambiente. Estas aplicaciones pueden facilitar la detección temprana de amenazas, permitir una respuesta rápida y agilizar las medidas de mitigación, además de ayudar a reforzar los regímenes de verificación del desarme.

Sin embargo, el uso de sensores también introduce una serie de retos singulares que deben abordarse. Los sensores, especialmente aquellos que intervienen en el intercambio de datos entre distintos sistemas, dependen en gran medida de las redes y son, por tanto, susceptibles de sufrir ciberataques. Los agentes malintencionados pueden intentar alterar o manipular los sistemas de

⁴³ Eshel (2022).

⁴⁴ van Amerongen (2021).

⁴⁵ UK National Quantum Technologies Programme (n.d.).

⁴⁶ Coggins et al. (n.d.).

⁴⁷ UK Defence Science and Technology Laboratory (2022).

⁴⁸ Hamblen (2023).

⁴⁹ Avtar et al. (2021).

sensores, poniendo en peligro así la integridad de los datos, lo que a su vez se traduce en una toma de decisiones errónea. Con los avances en la tecnología, los sensores adquieren la capacidad de generar volúmenes de datos cada vez mayores dentro de los sistemas, lo que puede dar lugar a importantes retardos y afectar a la calidad de los datos⁵⁰. Ello puede dificultar la toma de decisiones militares, a menos que se disponga de una arquitectura de red mejorada. Por último, al recoger y almacenar información relacionada tanto con personal militar como civil, las aplicaciones de sensores pueden suscitar preocupaciones legítimas en lo que respecta a la privacidad de las personas y las prácticas de vigilancia.

Sensores: lo más destacado de 2023

- La fusión de datos de sensores, consistente en integrar datos procedentes de diversas fuentes (como sensores acústicos, de radar o infrarrojos), proporciona un conocimiento exhaustivo del campo de batalla.
- La detección cuántica resulta prometedora para las aplicaciones militares, dado que aprovecha la sensibilidad de los estados cuánticos a las perturbaciones, lo que permite mediciones más precisas, la detección de objetos que se encuentran detrás de barreras y la mejora de los sistemas de navegación inercial en entornos sin señal GNSS. La integración de sensores con tecnologías de IA mejora la recopilación y el análisis de datos, lo que redundará en la toma de decisiones militares.
- La tecnología de sensores avanzados puede contribuir a los esfuerzos de seguridad internacional, ayudando a la vigilancia de conflictos armados en curso y el cumplimiento de los acuerdos de paz, así como a la detección temprana de sustancias peligrosas. No obstante, es esencial abordar los problemas de ciberseguridad y otros retos, como los posibles retardos derivados del aumento del volumen de datos.

4. Categoría III: Procesamiento y computación

4.1 Computación en la nube

*La **computación en la nube** brinda a los usuarios acceso a los recursos informáticos sin necesidad de mantener una infraestructura local. También ofrece flexibilidad para ampliar los recursos a medida que cambian las necesidades.*

La computación en la nube funciona con el respaldo de los componentes integrados de *hardware* y *software* de la infraestructura de nube⁵¹. En los últimos años, las capacidades de la computación en la nube han servido de catalizador para la innovación en un amplio espectro de aplicaciones, como el análisis de macrodatos, el aprendizaje automático, la computación sin servidor, la realidad

⁵⁰ Macri (2022).

⁵¹ Véase en el apartado 5.3 un análisis detallado de la infraestructura en la nube y los últimos avances.

aumentada (RA), la realidad virtual (RV) y otras tecnologías de vanguardia. Las plataformas basadas en la nube permiten ahora la externalización de la IA como servicio (AlaaS) y, por ende, el acceso generalizado a las capacidades transformadoras de la IA⁵². Además, la tecnología nativa de la nube se perfila como un enfoque novedoso para crear, probar, desplegar y gestionar aplicaciones en entornos de computación en la nube con las ventajas que brindan la escalabilidad, la mayor eficiencia y la reducción de costes⁵³.

La computación en la nube alberga potencial para impulsar la innovación en el sector militar. En concreto, el uso de la tecnología en la nube puede acelerar los procesos de diseño, desarrollo y pruebas de *software* para sistemas militares⁵⁴. Esto puede ampliar las capacidades en diversas aplicaciones militares, desde la inteligencia artificial y el aprendizaje automático hasta la modernización del *software* y la ciberseguridad⁵⁵. En el ámbito de la formación militar, las plataformas basadas en la nube pueden proporcionar al personal acceso a entornos de formación realistas e inmersivos, gracias a tecnologías emergentes como la RV o la RA. Desde septiembre de 2022, el ejército británico colabora con una empresa privada para desarrollar y ampliar una simulación inmersiva de guerra terrestre distribuida en la nube diseñada para facilitar el entrenamiento colectivo a gran escala de usuarios físicos y virtuales en varios emplazamientos⁵⁶. Asimismo, la computación en la nube proporciona la potencia de computación de alta velocidad necesaria para gestionar el procesamiento de datos a gran escala en operaciones militares. Dada la complejidad y el enorme volumen de los datos militares, la tecnología en la nube permite desplegar herramientas con las que las fuerzas armadas pueden analizar los datos con mayor eficacia. De este modo, pueden anticiparse a las amenazas en rápida evolución, manteniendo al mismo tiempo la seguridad⁵⁷.

No obstante, la tecnología en la nube conlleva posibles amenazas y retos. La integración de la computación en la nube en las operaciones militares suscita preocupación por lo que respecta a la seguridad de los datos, en particular cuando intervienen proveedores de servicios en la nube (CSP) externos⁵⁸. Además, los problemas de conectividad, como la elevada latencia en entornos remotos o difíciles, pueden afectar a la fiabilidad de los servicios basados en la nube y, por tanto, repercutir en la eficiencia operativa y la toma de decisiones en tiempo real. Por último, la mayor competencia mundial en el ámbito de la tecnología en la nube puede convertirse en un catalizador de una mayor tensión internacional, ya que los Estados podrían tratar de endurecer los controles a la exportación de tecnologías avanzadas en la nube atendiendo a sus intereses de seguridad nacional⁵⁹.

⁵² Marr (2023).

⁵³ Google (n.d.) and AWS (n.d.)

⁵⁴ Microsoft (2023).

⁵⁵ US Department of Defense (2023).

⁵⁶ Hadean (2022).

⁵⁷ Microsoft (2023).

⁵⁸ Véase en el apartado 5.3 un análisis más detallado de los problemas de seguridad de los datos asociados a la tecnología en la nube.

⁵⁹ Hayashi and McKinnon (2023).

Computación en la nube: lo más destacado de 2023

- La computación en la nube sigue impulsando la innovación en una serie de aplicaciones de última generación, como el análisis de macrodatos, el aprendizaje automático, la computación sin servidor, la RA y la RV. Las plataformas basadas en la nube permiten actualmente la externalización de la IA como servicio (AlaaS) democratizando el acceso a las capacidades transformadoras de la IA.
- En el sector militar, la tecnología en la nube puede facilitar entornos de formación realistas e inmersivos habilitados por tecnologías emergentes como la RV o la RA. La computación en la nube también proporciona potencia de computación de alta velocidad esencial para el procesamiento de datos a gran escala en operaciones militares. Sin embargo, los problemas de conectividad, como la elevada latencia en entornos remotos, pueden repercutir en la fiabilidad de los servicios basados en la nube.

4.2 Computación perimetral

***La computación perimetral** emplea un paradigma de computación distribuida consistente en reubicar el almacenamiento de datos y la computación más cerca de la fuente de datos —en el “borde” o la periferia— de la red, en lugar de depender de un sistema centralizado basado en la nube.*

En la computación perimetral, el procesamiento de datos se produce en un dispositivo o un servidor local situado en el “borde” o la periferia de una red. Cuando los datos requieren procesamiento en un centro de datos centralizados en la nube, solo se transmite la información estrictamente necesaria⁶⁰. Como resultado, la computación perimetral minimiza la latencia y mejora la potencia de computación, al almacenar y procesar los datos localmente y aliviar los posibles cuellos de botella de las redes en la nube y los centros de datos. Estas ventajas adquieren especial relevancia cuando los dispositivos en la computación perimetral requieren procesamiento en tiempo real, como ocurre con aplicaciones como Internet de las cosas, los vehículos autónomos y la RA.

El desarrollo de la computación perimetral podría transformar las operaciones del sector militar, mejorando las capacidades de comunicación, procesamiento de datos y toma de decisiones⁶¹. El despliegue de la computación perimetral sobre el terreno permite el intercambio instantáneo de datos entre fuerzas conectadas dentro de la misma red de borde, lo que facilita la comunicación y la coordinación en tiempo real. También lleva los recursos de computación al perímetro táctico de las operaciones militares y reduce la dependencia de los centros de datos en la nube. Los grandes conjuntos de datos sobre el terreno, como los obtenidos por sensores y los procedentes

⁶⁰ Microsoft Azure (n.d.).

⁶¹ Lee et al. (n.d.).

de vídeos de vigilancia y reconocimiento, pueden analizarse localmente en ubicaciones periféricas, lo que acelera los tiempos de respuesta y mejora la conciencia situacional. La adopción de una arquitectura de borde en el campo de batalla puede, por tanto, mejorar las aplicaciones de Internet de las cosas militares (IoMT) y permitir al personal militar reaccionar rápidamente ante situaciones potencialmente peligrosas⁶².

La computación perimetral garantiza la disponibilidad de recursos de datos y computación en emplazamientos remotos con conectividad intermitente a Internet, e incluso en entornos operativos extremos. Los análisis avanzados de IA pueden ejecutarse eficazmente en plataformas periféricas cuando están completamente desconectadas en entornos difíciles, lo que resulta de gran ayuda en misiones críticas como las operaciones de búsqueda y rescate⁶³. Sin embargo, las aplicaciones de IA desplegadas en dispositivos militares periféricos, como vehículos aéreos no tripulados, satélites y vehículos terrestres, suelen verse afectadas por limitaciones y pueden ofrecer un rendimiento menor que los modelos más avanzados debido a restricciones en la velocidad de procesamiento, la memoria de trabajo y la potencia⁶⁴. Asimismo, Amazon Web Services presentó recientemente AWS Snowblade, un nuevo producto de computación perimetral diseñado específicamente para el contrato Joint Warfighting Cloud Capability (JWCC) con el Departamento de Defensa de los Estados Unidos (DOD)⁶⁵. AWS Snowblade permite a los usuarios militares del JWCC realizar operaciones en emplazamientos en los que pueden darse temperaturas, vibraciones o impactos extremos.

Sin embargo, la computación perimetral conlleva ciertos retos de seguridad para las aplicaciones militares. El marco de computación distribuida puede aumentar la superficie de ataque, proporcionando más puntos finales para los ciberataques. La computación perimetral es vulnerable a una serie de amenazas de ciberseguridad, como los ataques de denegación de servicio (DoS), los ataques de canal lateral, los ataques de inyección de *malware* y los ataques de autenticación y autorización⁶⁶. Las instalaciones en la computación perimetral también están expuestas a daños físicos, lo que puede provocar alteraciones y filtraciones de datos en las redes de borde⁶⁷. Para hacer frente a estas vulnerabilidades, se están realizando esfuerzos continuos conducentes a mejorar las medidas de seguridad de los sistemas de la computación perimetral. Por ejemplo, los dispositivos periféricos de AWS Snowblade incorporan tecnología de cifrado avanzada para garantizar la seguridad de los datos y evitar el acceso no autorizado de posibles adversarios⁶⁸.

⁶² Cameron (2018).

⁶³ Thomas (2021).

⁶⁴ Miller and Lohn (2023).

⁶⁵ AWS (2023).

⁶⁶ Xiao et al. (2019).

⁶⁷ NATO CCDCOE (2022).

⁶⁸ Konkel (2023).

Computación perimetral: lo más destacado de 2023

- La computación perimetral, o *Edge computing*, tiene el potencial de transformar las operaciones militares, mejorando las capacidades de comunicación, procesamiento de datos y toma de decisiones. Además, en entornos remotos o extremos, la computación perimetral desempeña un papel fundamental a la hora de proteger los datos y proporcionar los recursos computacionales necesarios.
- Las plataformas periféricas permiten que los análisis de IA se realicen eficientemente sin conexión en entornos complejos, lo que resulta de gran ayuda en misiones críticas como las operaciones de búsqueda y rescate. Las limitaciones en la velocidad de procesamiento, la memoria y la potencia pueden afectar a las aplicaciones de IA en dispositivos militares de última generación.
- Los retos de seguridad persistentes que afectan a la computación perimetral en el ámbito militar incluyen mayor superficie para ciberataques y la vulnerabilidad a los daños físicos. Se están llevando a cabo esfuerzos continuos para mejorar las medidas de seguridad, como el cifrado avanzado en AWS Snowblade.

4.3 Computación cuántica⁶⁹

La computación cuántica es un campo emergente que aprovecha los principios de la mecánica cuántica para abordar problemas cuya complejidad supera las capacidades de los ordenadores clásicos.

El potencial de los ordenadores cuánticos para superar a los clásicos reside en fenómenos cuánticos únicos, en particular, la superposición y el entrelazamiento. Los bits cuánticos o cúbits, la unidad fundamental de información en computación cuántica, pueden existir simultáneamente en múltiples estados (0 y 1) debido a la superposición. Cuando los cúbits se entrelazan, el estado de un cúbit se vincula directamente al estado de otro, independientemente de la distancia física que exista entre ellos. El entrelazamiento cuántico puede aprovecharse para lograr aumentos significativos de la velocidad computacional, lo que permite a los ordenadores cuánticos realizar cálculos específicos de forma más eficiente que sus homólogos clásicos.

El campo de la computación cuántica ha experimentado avances considerables. Empresas privadas como IBM, Google/Alphabet y Microsoft han invertido grandes sumas en la investigación y el desarrollo de ordenadores cuánticos con utilidad práctica. IBM, por ejemplo, ha aumentado

⁶⁹ Un próximo informe del UNIDIR titulado “International Security in a Quantum New World: A Primer” ofrecerá un análisis más profundo sobre el campo de la computación cuántica y sus implicaciones en lo que respecta a la seguridad internacional.

constantemente el número de cúbits en un solo chip. En diciembre de 2023, IBM presentó el procesador Condor, que cuenta con 1.121 cúbits y representa un notable avance respecto al anterior procesador Osprey, de 433 cúbits⁷⁰. Al mismo tiempo, la empresa lanzó Heron, su procesador cuántico de mayor rendimiento hasta la fecha, equipado con 133 cúbits de alta calidad⁷¹. Cabe destacar que los procesadores Heron tienen capacidad para conectarse directamente con otros procesadores Heron, lo que podría facilitar la escalabilidad de los ordenadores cuánticos⁷².

Sin embargo, a pesar de estos avances, este campo sigue afrontando importantes retos aún sin resolver. Uno de los principales problemas es la decoherencia, un fenómeno cuántico resultante del aislamiento insuficiente de un cúbit físico con respecto a su entorno, lo cual puede introducir ruido en los cálculos. Así pues, superar la decoherencia y corregir los errores cuánticos se han convertido en cuestiones de importancia crítica⁷³. Asimismo, aunque las demostraciones matemáticas apuntan a las ventajas de los modelos cuánticos sobre los clásicos, aún no se dispone de suficientes pruebas empíricas debido a la falta de ordenadores cuánticos con un número suficiente de cúbits⁷⁴. Por ejemplo, los investigadores han calculado que para descifrar la criptografía más avanzada en ocho horas serían necesarios 20 millones de cúbits⁷⁵.

Aunque las aplicaciones prácticas de la computación cuántica siguen sin materializarse, los posibles avances futuros tienen una tremenda trascendencia para las prácticas militares y la seguridad internacional. La computación cuántica podría revolucionar diversos ámbitos tecnológicos, sobre todo en lo que respecta a la mejora de la inteligencia artificial y el aprendizaje automático. El éxito de los algoritmos clásicos de aprendizaje automático depende a menudo de parámetros amplios y una cantidad significativa de datos de entrenamiento. En cambio, con el aprendizaje automático cuántico es posible reducir el número de parámetros y datos necesarios, al aprovechar los diversos estados de que disponen las partículas cuánticas⁷⁶. La investigación empírica ha demostrado que las redes híbridas, que combinan características de los ordenadores clásicos y cuánticos, pueden ofrecer un mejor entrenamiento de los modelos de aprendizaje automático⁷⁷. Estos avances podrían transformar las futuras aplicaciones militares de la IA, especialmente en lo que se refiere al desarrollo de sistemas de armas autónomos letales más precisos⁷⁸.

Además, la computación cuántica puede redefinir el panorama de la ciberseguridad, lo cual conlleva tanto retos como oportunidades. Los ordenadores cuánticos son capaces de resolver ciertos problemas matemáticos exponencialmente más rápido que los ordenadores clásicos, lo que podría poner en peligro la seguridad de algunos algoritmos criptográficos de uso común

⁷⁰ Gambetta (2023).

⁷¹ Ibid.

⁷² Brooks (2023a).

⁷³ Lidar (2023).

⁷⁴ Brooks (2023b).

⁷⁵ Ibid.

⁷⁶ Ibid.

⁷⁷ Xu (2023).

⁷⁸ US Congressional Research Service (2023).

(como los sistemas de cifrado RSA y ECC). Se han desarrollado algoritmos cuánticos capaces de descifrar comunicaciones digitales, entre los que destaca el algoritmo de Shor, que podrán ejecutarse cuando se disponga de ordenadores cuánticos con utilidad práctica⁷⁹. Ello conlleva nuevas vulnerabilidades de ciberseguridad y puede dar lugar a ataques de tipo “recopilar ahora, descifrar después” (HNDL, por sus siglas en inglés), con los que los agentes malintencionados adquieren en el presente datos sensibles cifrados con la intención de descifrarlos más adelante, cuando lo permitan posibles avances en la tecnología de descifrado. Estos ataques pueden plantear problemas de seguridad nacional, al permitir a agentes hostiles acceder a información militar sensible⁸⁰. En respuesta a las posibles amenazas cuánticas, se están destinando esfuerzos al desarrollo de la criptografía poscuántica (PQC). El objetivo es crear sistemas criptográficos que puedan resistir futuros ataques de ordenadores cuánticos. Las tecnologías cuánticas emergentes, como la distribución cuántica de claves (QKD)⁸¹ y la generación cuántica de números aleatorios (QRNG)⁸², también ofrecen la oportunidad de mejorar los mecanismos de cifrado y las comunicaciones seguras.

Computación cuántica: lo más destacado de 2023

- La computación cuántica ha avanzado notablemente. IBM, por ejemplo, ha aumentado constantemente el número de cúbits en un solo chip, alcanzando un hito con la introducción del procesador Condor de 1.121 cúbits en 2023. Simultáneamente, la empresa lanzó el procesador Heron, capaz de conectarse directamente con otros procesadores Heron, lo que puede aportar una mayor escalabilidad.
- La investigación empírica ha demostrado que podría mejorarse el entrenamiento de modelos de aprendizaje automático mediante redes híbridas que combinen ordenadores clásicos y cuánticos. Este avance es de gran trascendencia para las aplicaciones de IA en el ámbito militar, en particular para el desarrollo de sistemas de armas autónomos letales más precisos.
- Sin embargo, el desarrollo de la computación cuántica plantea importantes retos para la ciberseguridad y la seguridad de la información; cabe destacar el riesgo de ataques del tipo “recopilar ahora, descifrar después”, dado el potencial de los ordenadores cuánticos con utilidad práctica para poner en peligro la seguridad de los algoritmos criptográficos de uso generalizado. En consecuencia, se están destinando esfuerzos a desarrollar la criptografía poscuántica para hacer frente a las amenazas cuánticas emergentes.

⁷⁹ van Amerongen (2021).

⁸⁰ US Congressional Research Service (2023).

⁸¹ NATO (2022).

⁸² Argillander et al. (2023).

5. Categoría IV: Infraestructura

5.1 5G y 6G

***5G** son las siglas empleadas para referirse a la quinta generación de tecnologías de redes móviles, que proporciona conexiones avanzadas de banda ancha superiores a las tecnologías predecesoras, como el 4G LTE. **6G** se refiere al desarrollo en curso de la sexta generación de tecnologías de redes móviles, diseñada para superar al 5G gracias a capacidades de red aún más avanzadas.*

La actual generación de infraestructuras de conectividad se caracteriza por aportar importantes avances en la tecnología inalámbrica, en particular la implantación generalizada de redes móviles de quinta generación (5G). La tecnología 5G presenta varias ventajas respecto a sus predecesoras, gracias a nuevas características como el segmentación de red —o *slicing*— y la capacidad de operar en el espectro de ondas milimétricas (mmWave), una banda de alta frecuencia del espectro radioeléctrico en el rango de 30-300 GHz⁸³. El 5G mejora significativamente la conectividad al proporcionar mayor velocidad, reducir la latencia, mejorar la fiabilidad de la red y permitir la conexión simultánea de un mayor número de dispositivos. Estas capacidades innovadoras del 5G son fundamentales para satisfacer la creciente demanda de innovaciones tecnológicas, especialmente en aplicaciones basadas en IoT, ya que permiten la conexión de más dispositivos y objetos a las redes.

La tecnología 5G ofrece un inmenso potencial para las aplicaciones militares transformadoras, facilitando una comunicación mejorada, una rápida transferencia de datos y la toma de decisiones en tiempo real en el campo de batalla. Su capacidad de conectividad de alta velocidad y baja latencia puede dar soporte a funciones militares críticas en los ámbitos de las comunicaciones y la logística, la ISR y el mando y control. Investigaciones recientes han puesto de relieve tres aplicaciones militares concretas posibles gracias a la implantación del 5G: el seguimiento de artículos y equipos mediante etiquetas inteligentes para mejorar las operaciones; la utilización de las redes 5G de banda ancha para la transferencia de grandes conjuntos de datos de sensores; y el uso de comunicaciones 5G remotas con fines de mando y control para mejorar la coordinación multinacional⁸⁴. El seguimiento mediante etiquetas inteligentes en los envíos a través de una red 5G también puede contribuir a los esfuerzos de control de armas, gracias a su potencial para mitigar los riesgos asociados con el desvío de armas y municiones convencionales. Asimismo, el 5G puede actuar como potente catalizador para las aplicaciones más avanzadas de IA e IoT en el ámbito militar y poner los cimientos de la mejora de las capacidades. Las redes 5G de alta velocidad pueden facilitar la integración de la IA para el procesamiento eficiente de ingentes cantidades de datos de sensores en el campo de batalla. Así, las señales de adversarios pueden transmitirse en tiempo real a través de una red 5G segura para su posterior análisis mediante algoritmos avanzados de procesamiento de señales⁸⁵.

⁸³ Gerwig and Goss. (2023).

⁸⁴ Lee et al. (2023).

⁸⁵ Tucker (2022).

Sin embargo, la integración de la tecnología 5G comporta nuevos riesgos, en particular en el ámbito de la ciberseguridad. Con el aumento de los volúmenes de datos y los dispositivos interconectados en las redes 5G pueden agravarse las posibles vulnerabilidades de seguridad, lo que ofrece a los agentes maliciosos más oportunidades para la explotación y la interrupción. Las características de la tecnología 5G, incluidas las interfaces abiertas y su naturaleza basada en la nube, también crean riesgos adicionales para la seguridad, dando lugar a un panorama de amenazas expansivo asociado a su despliegue⁸⁶. Una gran variedad de amenazas a la ciberseguridad pueden manifestarse a través de los múltiples subsistemas 5G, que abarcan los equipos de usuario 5G y la red de acceso radioeléctrico (RAN), la red troncal, los servicios en la nube y la computación perimetral de acceso múltiple (MEC), entre otros componentes críticos⁸⁷.

Actualmente se están desarrollando las redes móviles 6G, que traerán consigo aún más avances que la actual tecnología 5G. Se espera que aporten nuevas mejoras en cuanto a velocidad, latencia y conectividad y hagan posible una gama más amplia de aplicaciones tecnológicas novedosas. En comparación con las anteriores generaciones de redes de comunicaciones, los esfuerzos de investigación y desarrollo del 6G se orientan más a lograr una cobertura de red integral “en tierra, mar, aire y espacio”, combinando redes móviles terrestres con plataformas aéreas y por satélite⁸⁸. Esta arquitectura integrada de red satelital-terrestre alberga un gran potencial para garantizar la cobertura mundial de Internet y proporcionar un soporte de comunicación ubicuo para Internet de las cosas⁸⁹. Se espera que el despliegue de la tecnología 6G comience en torno al año 2030⁹⁰.

5G y 6G: lo más destacado de 2023

- Los avances actuales de la tecnología 5G ofrecen un gran potencial transformador a las aplicaciones militares que permitirá mejorar las comunicaciones, agilizar la transferencia de datos y tomar decisiones en tiempo real en el campo de batalla. El 5G también puede facilitar la integración de aplicaciones punteras de IA e IoT, mejorando así las capacidades militares.
- Sin embargo, la introducción de la tecnología 5G amplifica las posibles vulnerabilidades de ciberseguridad debido al aumento en el volumen de datos y los dispositivos interconectados. Las interfaces abiertas y su naturaleza basada en la nube también dan lugar a un amplio panorama de amenazas asociado a los despliegues 5G.
- La investigación y el desarrollo en curso de las redes móviles 6G se centran en lograr una cobertura completa en tierra, mar, aire y espacio mediante una red integrada satelital-terrestre cuyo despliegue se prevé para 2030.

⁸⁶ Śliwa and Suchański (2022).

⁸⁷ NATO CCDCOE (2022).

⁸⁸ Chen et al. (2023).

⁸⁹ Tirmizi et al. (2022).

⁹⁰ Kharpal (2023) and Chen et al. (2023).

5.2 Internet de las cosas

*El **Internet de las cosas (IoT)** permite vincular una extensa red de dispositivos físicos, electrodomésticos, vehículos y otros objetos que constan de sensores, software y conectividad de red, facilitando la recopilación y el intercambio de datos entre dispositivos y sistemas. Al permitir que estos dispositivos se comuniquen y colaboren entre sí a través de Internet u otras redes de comunicaciones, IoT crea un ecosistema interconectado que puede supervisarse y controlarse a distancia.*

Los recientes avances en el ámbito de Internet de las cosas (IoT) están íntimamente relacionados con las innovaciones tecnológicas en otras áreas, en particular la computación perimetral, las redes 5G y la integración de la inteligencia artificial⁹¹. El auge de la computación perimetral ha dado lugar a un enfoque más localizado del procesamiento y almacenamiento de datos, lo que a su vez ha permitido reducir eficazmente la latencia y mejorar las capacidades de procesamiento en tiempo real de los dispositivos IoT⁹². Por su parte, el despliegue de las redes 5G también ha acelerado el desarrollo de IoT, al agilizar la transferencia de datos, reducir la latencia y ampliar la capacidad de la red⁹³. Además, la integración de tecnologías de IA, en concreto el aprendizaje automático, da soporte al análisis y la interpretación en tiempo real de la gran cantidad de datos generados por las aplicaciones IoT, lo que se traduce en una toma de decisiones y una automatización más eficientes.

La tecnología IoT se utiliza cada vez más en los sistemas militares para optimizar las operaciones y mejorar la eficiencia, lo que ha facilitado la transición a un entorno militar más conectado y basado en datos. El Internet de las cosas militares (IoMT) puede emplear un conjunto diverso de sensores desplegados en varios dominios, con el objetivo de lograr una conciencia situacional integral y un control eficaz en entornos de conflicto complejos y diversos⁹⁴. La incorporación de redes de sensores y sistemas no tripulados en el marco de IoMT puede mejorar significativamente las capacidades de vigilancia y reconocimiento, permitiendo a las fuerzas armadas rastrear el entorno del campo de batalla, gestionar equipos y vehículos y controlar el estado de salud de los soldados⁹⁵. El uso de la tecnología IoT/IoMT puede aportar mayor precisión en la selección de objetivos y minimizar el riesgo de bajas civiles durante las operaciones militares, ya que los sensores integrados en una red IoT/IoMT pueden guiar las armas con mayor precisión hacia el objetivo previsto⁹⁶.

Asimismo, los avances en la tecnología IoT/IoMT también han mejorado significativamente los sistemas de comunicaciones militares. La IoT facilita el intercambio de datos y la conectividad sin fisuras, mejorando así la colaboración entre las fuerzas conjuntas y de la coalición y entre distintos dominios⁹⁷. Además, la integración de protocolos de comunicaciones seguras y el uso de cifrado y

⁹¹ Coughlin (2023).

⁹² Véase en el apartado 4.2 un análisis detallado de la computación perimetral y sus últimos avances.

⁹³ Véase en el apartado 5.1 un análisis detallado de las redes móviles 5G y los últimos avances.

⁹⁴ Withrington (2023).

⁹⁵ Khawaja (2023).

⁹⁶ Douglass (2022).

⁹⁷ Breaking Defense (2023).

firmas digitales en los sistemas habilitados por IoT permiten salvaguardar eficazmente los canales de comunicación, garantizando la confidencialidad, integridad y disponibilidad de la información militar sensible⁹⁸. No obstante, sin protocolos de comunicación robustos, la adopción generalizada de la tecnología IoT puede conllevar serias amenazas a la ciberseguridad de los sistemas militares interconectados. Las redes IoMT presentan una gran superficie de ataque que comprende los dispositivos IoMT, los canales de comunicación que conectan estos dispositivos, las aplicaciones *back-end* específicas de IoMT y el almacenamiento de datos *back-end*⁹⁹. Las repercusiones de las operaciones cibernéticas en las que intervienen dispositivos IoT pueden trascender a los sistemas militares y llegar a provocar interrupciones indiscriminadas en otros sistemas conectados, como instalaciones médicas, instituciones educativas y otras redes sensibles¹⁰⁰.

Internet de las cosas: lo más destacado de 2023

- La tecnología IoT se aplica cada vez más en los sistemas militares con fines de optimización operativa (lo que se conoce como “Internet de las cosas militares”). IoMT emplea una amplia gama de sensores en todos los ámbitos para obtener una conciencia situacional y control exhaustivos. Los sensores integrados en una red IoT/IoMT también pueden mejorar la precisión de los objetivos en operaciones militares, así como minimizar el riesgo de bajas civiles.
- Sin embargo, en ausencia de protocolos de comunicación robustos, la adopción generalizada de IoT en sistemas militares puede plantear riesgos en el ámbito de la ciberseguridad. Las redes IoMT crean una importante superficie de ataque cuyas posibles repercusiones pueden trascender a los sistemas militares y afectar a otros sectores críticos, como instalaciones médicas, instituciones educativas y otras redes sensibles.

5.3 Infraestructura en la nube

La infraestructura en la nube consta de componentes de hardware y software esenciales para prestar servicios en la nube a través de Internet. El hardware incluye servidores, almacenamiento, componentes de red y centros de datos, y el software elementos como los programas informáticos de virtualización.

La infraestructura en la nube proporciona la base sobre la que se construyen y prestan los servicios de computación en la nube¹⁰¹. Los servicios en la nube han vivido un auge en los últimos años, y las empresas privadas desempeñan un papel fundamental como proveedores de servicios en la

⁹⁸ Kannan et al. (2023).

⁹⁹ Withrington (2023).

¹⁰⁰ Renals (2021).

¹⁰¹ Véase en el apartado 4.1 un análisis detallado de la computación en la nube y sus últimos avances.

nube (CSP). Entre los principales CSP figuran Amazon Web Services (AWS), Microsoft Azure, Google Cloud, Oracle Cloud y Alibaba Cloud. Ofrecen una amplia gama de servicios en la nube que pueden agruparse en tres categorías principales: infraestructura como servicio (IaaS), plataforma como servicio (PaaS) y software como servicio (SaaS). Los CSP han seguido ampliando rápidamente la cobertura de su infraestructura de nube en todo el mundo y se han hecho presentes en todos los continentes¹⁰².

La tecnología en la nube se utiliza cada vez más para adquirir una mayor eficiencia operativa y mejorar la gestión de datos en contextos militares. Las fuerzas armadas no solo han desarrollado su infraestructura interna en la nube, sino que también han adoptado capacidades y servicios comerciales en la nube de CSP privados. Por ejemplo, en diciembre de 2022, el Departamento de Defensa de los Estados Unidos (DOD) adjudicó contratos a cuatro grandes CSP —AWS, Google, Microsoft y Oracle— para dar soporte a su Joint Warfighting Cloud Capability¹⁰³. La infraestructura en la nube permite a las fuerzas armadas almacenar y gestionar grandes volúmenes de datos militares, tales como datos de ISR, información logística y otros datos esenciales. Esto puede facilitar la comunicación y la coordinación entre el personal militar y las unidades destacadas en diversos emplazamientos.

Garantizar la seguridad de los datos ha sido una cuestión esencial para el despliegue de la tecnología en la nube en contextos militares. La infraestructura en la nube suele ofrecer mayor seguridad para la información sensible, gracias a un cifrado robusto, a la gestión de identidades y accesos y a otras funciones de seguridad avanzadas. En particular, la decisión proactiva del Gobierno ucraniano de migrar una parte significativa de sus datos críticos a la nube contribuyó sensiblemente a la preparación del país para resistir a ciberataques sin precedentes¹⁰⁴. Tanto los gobiernos como los CSP han seguido reforzando las medidas de seguridad de su infraestructura en la nube y han adoptado un enfoque de confianza cero en los entornos de computación en la nube¹⁰⁵.

No obstante, los entornos en la nube, al igual que otras plataformas digitales, siguen estando expuestos a posibles vulnerabilidades y riesgos cibernéticos. La transferencia de datos confidenciales a sistemas en la nube comporta mayores riesgos para la seguridad, como demuestran incidentes pasados de seguridad en la nube. En febrero de 2023, un volumen considerable de correos electrónicos militares confidenciales quedó expuesto debido a un servidor de correo electrónico mal configurado en la plataforma Microsoft Azure Government Cloud.¹⁰⁶ Aunque la utilización de servicios comerciales en la nube prestados por los principales CSP ofrece las ventajas de contar con unos protocolos de seguridad sólidos y una elevada concentración de conocimientos especializados, también conlleva la posibilidad de que los incidentes que afecten a la infraestructura en la nube de dichos proveedores tengan efectos

¹⁰² Mapa global de la infraestructura en la nube de ocho grandes proveedores de servicios en la nube:

<https://www.cloudinfrastructuremap.com/>

¹⁰³ US Department of Defense (2022).

¹⁰⁴ Lewis (2023).

¹⁰⁵ US Department of Defense (2023).

¹⁰⁶ Martin et al. (2023).

generalizados¹⁰⁷. Además, el Comité Internacional de la Cruz Roja (CICR) ha destacado la creciente participación de civiles en operaciones digitales durante los conflictos armados, lo que podría conducir a un mayor uso de la infraestructura civil, incluida la infraestructura en la nube, con fines militares¹⁰⁸. Esta tendencia supone un mayor riesgo de que los civiles y las infraestructuras civiles sean blanco de ataques, lo que socava el principio de distinción, respaldado por todos los países¹⁰⁹.

Infraestructura en la nube: lo más destacado de 2023

- Las fuerzas armadas utilizan cada vez más las infraestructuras en la nube para mejorar la eficiencia operativa y la gestión de datos. Aunque se están aplicando medidas de seguridad avanzadas, como un cifrado robusto, la integración de entornos en la nube en contextos militares sigue sujeta a riesgos cibernéticos, como demuestran incidentes pasados.
- Además, el CICR ha puesto de relieve la creciente participación de civiles en operaciones digitales durante conflictos armados, lo que podría aumentar el uso de infraestructuras civiles, incluida la infraestructura en la nube, con fines militares. Ello a su vez supone un mayor riesgo de ataque a civiles e infraestructuras civiles, lo que contraviene el principio de distinción.

5.4 Comunicaciones por satélite

Las comunicaciones por satélite implican el uso de satélites artificiales para establecer conexiones de comunicación entre diversos emplazamientos de la Tierra.

Los sistemas de comunicaciones por satélite desempeñan un papel fundamental a la hora de garantizar la cobertura mundial de Internet, cerrar la brecha digital y aumentar la resiliencia de las infraestructuras de conectividad, especialmente en zonas donde las redes de comunicaciones terrestres tradicionales son limitadas o no están disponibles. Las tecnologías de satélites forman parte integrante de las operaciones militares, y los continuos avances en este campo siguen impulsando la innovación en el sector de la defensa. El actual auge de las constelaciones de satélites en órbita terrestre baja (OTB) previsiblemente aumentará de forma considerable el número de satélites en órbita alrededor de la Tierra. En comparación con los satélites geosincrónicos clásicos, las grandes constelaciones de satélites de menor tamaño en OTB pueden reducir sustancialmente la latencia, aumentar la capacidad de ancho de banda y ofrecer una cobertura mundial ininterrumpida. Son fundamentalmente entidades privadas las que están a la cabeza del desarrollo de satélites OTB, como Starlink de SpaceX, OneWeb y el Proyecto Kuiper de Amazon¹¹⁰.

¹⁰⁷ Maurer and Hinck (2020).

¹⁰⁸ ICRC (2023).

¹⁰⁹ Ibid.

¹¹⁰ Borowitz (2022).

Las fuerzas armadas pueden aprovechar la conectividad mejorada que proporcionan los sistemas OTB para efectuar transferencias de datos en tiempo real y aumentar así la precisión y eficiencia de las operaciones militares. Como se ha observado en el conflicto entre Rusia y Ucrania, la constelación de satélites OTB Starlink de SpaceX ha sido un facilitador fundamental de la comunicación crítica con fines civiles y militares en Ucrania, y se ha empleado en vehículos aéreos no tripulados de vigilancia y reconocimiento¹¹¹. Además de las aplicaciones de defensa, las constelaciones OTB también pueden ayudar a cerrar la brecha digital mundial, proporcionando Internet de alta velocidad en zonas remotas o rurales donde la infraestructura terrestre tradicional es difícil de desplegar¹¹².

Otra innovación notable en las comunicaciones por satélite es la integración de tecnologías cuánticas. La distribución cuántica de claves (QKD) puede proteger las comunicaciones por satélite aplicando los principios de la mecánica cuántica para crear e intercambiar claves de cifrado entre dos partes. En septiembre de 2022, la Agencia Espacial Europea anunció una colaboración con la Comisión Europea y más de 20 empresas del sector espacial europeo para introducir el primer sistema QKD basado en el espacio de la región, conocido como satélite Eagle-1¹¹³. Este sistema de conectividad vía satélite pondrá los cimientos de una red ultrasegura en Europa. Al mismo tiempo, países como China¹¹⁴ y Singapur¹¹⁵ están desarrollando la tecnología QKD para mejorar la seguridad de las comunicaciones por satélite.

Aunque la tecnología por satélite ofrece enormes posibilidades de conectividad global y comunicaciones seguras, también conlleva una serie de problemas de seguridad. Uno de estos escollos se debe a la susceptibilidad de los sistemas de satélites a las ciberamenazas y las posibles violaciones de la seguridad de los datos. Las comunicaciones por satélite son indispensables para transmitir información sensible crucial para las operaciones militares, y cualquier daño a estos sistemas puede acarrear importantes desventajas estratégicas. Los sistemas de comunicaciones militares por satélite se han convertido en blanco de ciberataques que provocan cortes y alteraciones en servicios críticos¹¹⁶. El despliegue de satélites en órbita, sobre todo los numerosos satélites OTB, también puede plantear problemas de seguridad, como los relacionados con el tráfico espacial y el aumento de los desechos espaciales, que suponen una amenaza para la seguridad y la sostenibilidad del espacio¹¹⁷. Por otra parte, habida cuenta del papel fundamental que desempeñan las entidades privadas en el campo de las comunicaciones por satélite, las fuerzas armadas seguirán utilizando las tecnologías comerciales en su beneficio. No obstante, la dependencia de agentes comerciales para las infraestructuras de comunicación críticas durante los conflictos ha puesto de relieve posibles dificultades derivadas de las diferencias existentes

¹¹¹ Jayanti (2023).

¹¹² Marquina (2022).

¹¹³ ESA (2022).

¹¹⁴ Laursen (2022).

¹¹⁵ SpeQtral (2022).

¹¹⁶ Menn (2023).

¹¹⁷ Mukherjee (2021).

entre las entidades privadas y públicas en lo que respecta a los incentivos, los principios operativos y los mecanismos de rendición de cuentas¹¹⁸.

Comunicaciones por satélite: lo más destacado de 2023

- Entre las innovaciones significativas en las comunicaciones por satélite destaca el aumento de las constelaciones de satélites OTB gestionadas por entidades privadas, como Starlink de SpaceX. Además de contribuir a mejorar la conectividad mundial, también resultan esenciales en las operaciones militares, al facilitar la comunicación crítica durante los conflictos. Por otra parte, la integración de la tecnología de distribución cuántica de claves en los sistemas de satélites sienta las bases de unas comunicaciones más seguras.
- No obstante, las comunicaciones por satélite también pueden plantear problemas de seguridad, como vulnerabilidades ante las ciberamenazas, y suscitar inquietud por motivo de los desechos espaciales. Asimismo, dado que las fuerzas armadas continúan utilizando tecnologías de satélites comerciales, resulta primordial destacar los posibles dificultades derivadas de las diferencias entre entidades públicas y privadas en lo que respecta a los incentivos, los principios operativos y los mecanismos de rendición de cuentas.

6. Conclusión

En todos los ámbitos tecnológicos examinados en este documento existen varias tendencias y desarrollos transversales. En particular, una tendencia consolidada observable en la tecnología de *hardware* es el proceso continuo de miniaturización, que conduce a la creación de dispositivos cada vez más pequeños y eficientes. Los recientes avances en materiales semiconductores, nanotecnología, microchips y sensores han resultado determinantes para este cambio transformador. Esta tendencia impulsa la adopción generalizada de tecnologías facilitadoras en los ámbitos del armamento y los sistemas militares, contribuyendo a la modernización de los equipos militares.

El aprovechamiento de las tecnologías facilitadoras aumentará notablemente diversas capacidades militares. Entre ellas se incluyen la mejora de la conciencia situacional, un mando y control optimizados, la aceleración de la transferencia y el procesamiento de datos y una mayor precisión del armamento avanzado. En particular, algunas tecnologías facilitadoras, como los microchips, la computación en la nube y la computación cuántica, actúan como catalizadores de la innovación en las aplicaciones militares. Facilitan la integración de tecnologías transformadoras, como la IA y las capacidades de aprendizaje automático, y amplían aún más el potencial de avances en las operaciones militares. Además, las tecnologías facilitadoras pueden potenciar los

¹¹⁸ Jayanti (2023).

esfuerzos internacionales de seguridad, reforzando los mecanismos de verificación del desarme y de supervisión de conflictos. Ello puede lograrse, por ejemplo, mediante el uso de sensores avanzados para detectar agentes químicos y biológicos en el medio ambiente, así como para vigilar el cumplimiento de los acuerdos de paz.

Sin embargo, los recientes avances en las tecnologías facilitadoras también plantean riesgos y retos significativos. Si bien las innovaciones en el ámbito de la tecnología en la nube y la distribución cuántica de claves pueden mejorar la seguridad de las comunicaciones, el almacenamiento de información y el procesamiento de datos, el despliegue a gran escala de tecnologías facilitadoras conlleva una mayor vulnerabilidad frente a los riesgos de ciberseguridad. Esta expansión del panorama tecnológico puede ampliar la superficie de ataque y dificultar la salvaguarda de los sistemas militares frente a posibles ciberamenazas. La computación cuántica, en particular, puede tener un efecto disruptivo en protocolos y normas de cifrado ampliamente utilizados debido a su capacidad inherente para descifrar códigos.

Además, la búsqueda de innovaciones de última generación en las tecnologías facilitadoras podría intensificar las tensiones internacionales y alentar la competencia tecnológica entre los Estados. Los Estados pueden tratar de imponer controles estrictos a la exportación de tecnologías avanzadas en consonancia con sus intereses de seguridad nacional. Además, las vulnerabilidades de la cadena de suministro constituyen un reto importante en el ámbito de las tecnologías facilitadoras. La cadena de suministro de componentes de *hardware*, como los microchips, es una red muy globalizada y compleja que presenta una elevada concentración de la producción especializada en determinadas regiones del planeta. Cualquier perturbación de las capacidades de fabricación en estas regiones, ya sea derivada de tensiones geopolíticas o de catástrofes naturales, repercutiría negativamente en la disponibilidad de las tecnologías y afectaría a la seguridad internacional.

Por último, los avances en muchos ámbitos tecnológicos ponen de relieve el papel fundamental que desempeña el sector privado. Las empresas privadas han impulsado el progreso y la innovación en un variado espectro de aplicaciones tecnológicas, como las tecnologías en la nube, las comunicaciones por satélite y la computación cuántica. Las fuerzas armadas llevan tiempo colaborando con entidades privadas para beneficiarse de las tecnologías más avanzadas, pero esta colaboración no está exenta de riesgos. Los incidentes que afectan a la infraestructura de empresas privadas pueden tener efectos generalizados y poner en riesgo información militar sensible. La dependencia de agentes privados también puede acarrear posibles desafíos derivados de las diferencias entre entidades privadas y públicas en lo que respecta a los incentivos, los principios de funcionamiento y los mecanismos de rendición de cuentas.

Los avances en las tecnologías facilitadoras seguirán ejerciendo un notable efecto en las prácticas militares y la seguridad internacional. Por este motivo, se precisa una continua exploración de horizontes para identificar tendencias nuevas y emergentes, así como un estudio de los posibles marcos de gobernanza para aprovechar las oportunidades y mitigar los riesgos. En futuros proyectos de investigación, el UNIDIR seguirá identificando y analizando tecnologías nuevas y emergentes, así como aplicaciones novedosas de tecnologías más establecidas. Asimismo,

proporcionará recomendaciones políticas orientadas a la acción destinadas a la gobernanza efectiva de las distintas categorías tecnológicas.

Referencias

Amazon Web Services (AWS). 2023. "Announcing AWS Snowblade for U.S. Department of Defense JWCC Customers". 6 June. Consultado el 6 de diciembre de 2023:

<https://aws.amazon.com/about-aws/whats-new/2023/06/aws-snowblade-us-defense-jwcc-customers/>

—.n.d. "What is cloud native?". Consultado el 6 de diciembre de 2023:

<https://aws.amazon.com/what-is/cloud-native/>

Arcuri, Gregory and Sujai Shivakumar. 2022. "Moore's Law and Its Practical Implications". Center for Strategic & International Studies. 18 October. Consultado el 6 de diciembre de 2023:

<https://www.csis.org/analysis/moores-law-and-its-practical-implications>

Argillander, Joakim et al. 2023. "Quantum Random Number Generation Based on a Perovskite Light Emitting Diode". *Communications Physics* 6, 157. Consultado el 6 de diciembre de 2023:

<https://doi.org/10.1038/s42005-023-01280-3>

ASML. n.d. "EUV Lithography Systems". Consultado el 6 de diciembre de 2023:

<https://www.asml.com/en/products/euv-lithography-systems>

Avtar, Ram et al. 2021. "Remote Sensing for International Peace and Security: Its Role and Implications". *Remote Sensing* 13, 3: 439. Consultado el 6 de diciembre de 2023:

<https://doi.org/10.3390/rs13030439>

Basheer, Taha et al. 2022. "Nanotechnology and Computer Science: Trends and Advances". *Memories - Materials, Devices, Circuits and Systems* 2, October. Consultado el 6 de diciembre de 2023: <https://doi.org/10.1016/j.memori.2022.100011>

Borowitz, Mariel. 2022. "The Military Use of Small Satellites in Orbit". French Institute of International Relations. 4 March. Consultado el 6 de diciembre de 2023:

https://www.ifri.org/sites/default/files/atoms/files/m._borowitz_military_use_small_satellites_in_orbit_03.2022.pdf

Breaking Defense. 2023. "When We Talk about What Will Enable JADC2, We're Really Talking about the Internet of Warfighting Things". 22 March. Consultado el 6 de diciembre de 2023:

<https://breakingdefense.com/2023/03/when-we-talk-about-what-will-enable-jadc2-were-really-talking-about-the-internet-of-warfighting-things/>

Brooks, Michael. 2023a. "What's Next for Quantum Computing". MIT Technology Review. 6 January. Consultado el 6 de diciembre de 2023:

<https://www.technologyreview.com/2023/01/06/1066317/whats-next-for-quantum-computing/>

Brooks, Michael. 2023b. "Quantum Computers: What are They Good For?". *Nature*. 24 May.

Consultado el 6 de diciembre de 2023: <https://www.nature.com/articles/d41586-023-01692-9>

Cameron, Lori. 2018. "Internet of Things Meets the Military and Battlefield: Connecting Gear and Biometric Wearables for an IoMT and IoBT". IEEE Computer Society. 1 March. Consultado el 6 de diciembre de 2023: <https://www.computer.org/publications/tech-news/research/internet-of-military-battlefield-things-iomt-iobt>

Chandler, David L. 2022. "The Best Semiconductor of Them All?". MIT News. 21 July. Consultado el 6 de diciembre de 2023: <https://news.mit.edu/2022/best-semiconductor-them-all-0721>

Chen, Zhi et al. 2023. "Experts' Take on 6G Technology". China Daily. 7 August. Consultado el 6 de diciembre de 2023: https://www.chinadaily.com.cn/a/202308/07/WS64d01ddca31035260b81a8d3_1.html

Clynes, Tom. 2023. "5 Big Ideas for High-Temperature Superconductors". IEEE Spectrum. 18 September. Consultado el 6 de diciembre de 2023: <https://spectrum.ieee.org/high-temperature-superconductors>

Coggins, Kevin et al. n.d. "Quantum Sensing: A New Approach to Maintaining PNT in GPS-Denied Environments". US Naval Institute. Consultado el 6 de diciembre de 2023: <https://www.usni.org/magazines/proceedings/sponsored/quantum-sensing-new-approach-maintaining-pnt-gps-denied>

Coughlin, Tom. 2023. "9 IoT Trends to Keep an Eye on in 2023 and Beyond". TechTarget. 12 July. Consultado el 6 de diciembre de 2023: <https://www.techtarget.com/iotagenda/opinion/IoT-trends-to-keep-an-eye-on>

Douglass, Robert. 2022. "Introduction: IoT for Defense and National Security". In IoT for Defense and National Security (eds R. Douglass, K. Gremban, A. Swami and S. Gerali). Consultado el 6 de diciembre de 2023: <https://doi.org/10.1002/9781119892199.fmatter>

Eshel, Tamir. 2022. "Sensor Fusion for Land Combat Vehicles". European Security & Defence. 26 April. Consultado el 6 de diciembre de 2023: <https://euro-sd.com/2022/04/articles/exclusive/25763/sensor-fusion-for-land-combat-vehicles/>

European Space Agency (ESA). 2022. "Quantum Encryption to Boost European Autonomy". 22 September. Consultado el 6 de diciembre de 2023: https://www.esa.int/Applications/Connectivity_and_Secure_Communications/Quantum_encryption_to_boost_European_autonomy

Fadelli, Ingrid. 2023. "Researchers Demonstrate Scaling of Aligned Carbon Nanotube Transistors to below Sub-10 nm Nodes". Phys.org. 27 July. As of 3 January 2024: <https://phys.org/news/2023-07-scaling-aligned-carbon-nanotube-transistors.html>

Feldman, Andrey. 2023. "New Superconductor Could Lead to Quantum Computing Breakthrough". Advanced Science News. 18 July. Consultado el 6 de diciembre de 2023: <https://www.advancedsciencenews.com/new-superconductor-could-lead-to-quantum-computing-breakthrough/>

Gambetta, Jay. 2023. "The Hardware and Software for the Era of Quantum Utility is Here". IBM. 4 December. As of 11 January: <https://www.ibm.com/quantum/blog/quantum-roadmap-2033>

Gargeyas, Arjun. 2022. "The Role of Semiconductors in Military and Defence Technology". *Defence and Diplomacy Journal* 11, 2 (January–March). Consultado el 6 de diciembre de 2023: <https://capsindia.org/wp-content/uploads/2022/07/DD-Journal-January-March-2022-Arjun-Gargeyas.pdf>

Gerwig, Kate and Michaela Goss. 2023. "The Essential 5G Glossary of Key Terms and Phrases". TechTarget. 19 October. Consultado el 6 de diciembre de 2023: <https://www.techtarget.com/searchnetworking/feature/The-essential-5G-glossary-of-key-terms-and-phrases>

Gilchrist, Karen. 2023. "How U.S. Microchips are Fueling Russia's Military – Despite Sanctions". CNBC. 7 August. Consultado el 6 de diciembre de 2023: <https://www.cnbc.com/2023/08/07/how-us-microchips-are-fueling-russias-military-despite-sanctions.html>

Giles, Martin. 2019. "Cybersecurity Flaws in Chips are Still Taking Too Long to Fix". MIT Technology Review. 3 June. Consultado el 6 de diciembre de 2023: <https://www.technologyreview.com/2019/06/03/135108/cybersecurity-flaws-in-chips-are-taking-too-long-to-fix/>

Google. n.d. "What is Cloud Native?". Consultado el 6 de diciembre de 2023: <https://cloud.google.com/learn/what-is-cloud-native>

Hadean. 2022. "Hadean Awarded British Army Contract to Build Simulation Pathfinder". 14 July. Consultado el 6 de diciembre de 2023: <https://hadean.com/news/hadean-awarded-british-army-contract-to-build-simulation-pathfinder/>

Hamblen, Matt. 2023. "Stephanie Brown on Sensors Worn by Soldiers for Their Vital Data". Fierce Electronics. 6 June. Consultado el 6 de diciembre de 2023: <https://www.fierceelectronics.com/sensors/tesla-recalls-2-million-cars-software-update-provide-visual-and-audible-alerts>

Hamza, Ekhlas Kadum and Shahad Nafea Jaafar. 2022. "Nanotechnology Application for Wireless Communication System". In *Nanotechnology for Electronic Applications. Materials Horizons: From Nature to Nanomaterials*. Springer, Singapore. Consultado el 6 de diciembre de 2023: https://doi.org/10.1007/978-981-16-6022-1_6

Hayashi, Yuka and John D. McKinnon. 2023. "U.S. Looks to Restrict China's Access to Cloud Computing to Protect Advanced Technology". 4 July. Consultado el 6 de diciembre de 2023: <https://www.wsj.com/articles/u-s-looks-to-restrict-chinas-access-to-cloud-computing-to-protect-advanced-technology-f771613>

Hecht, Jeff. 2022. "Nanomaterials Pave the Way for the Next Computing Generation". Nature. 10 August. Consultado el 6 de diciembre de 2023: <https://www.nature.com/articles/d41586-022-02147-3>

IBM. 2023. "Why We Need EUV Lithography for the Future of Chips". 26 June. Consultado el 6 de diciembre de 2023: <https://research.ibm.com/blog/what-is-euv-lithography>

Institute of Electrical and Electronics Engineers (IEEE). n.d.-a. "Future of Semiconductor Performance". Consultado el 6 de diciembre de 2023: <https://irds.ieee.org/topics/future-of-semiconductor-performance>

—.n.d.-b. "Semiconductor Materials". Consultado el 6 de diciembre de 2023: <https://irds.ieee.org/topics/semiconductor-materials>

Intel. n.d. "The Story of the Intel® 4004". Consultado el 6 de diciembre de 2023: <https://www.intel.com/content/www/us/en/history/museum-story-of-intel-4004.html>

Jayanti, Amritha. 2023. "Starlink and the Russia–Ukraine War: A Case of Commercial Technology and Public Purpose?". Analysis & Opinions, Belfer Center for Science and International Affairs, Harvard Kennedy School. 9 March. Consultado el 6 de diciembre de 2023: <https://www.belfercenter.org/publication/starlink-and-russia-ukraine-war-case-commercial-technology-and-public-purpose>

Kannan, B. Maruthu et al. 2023. "Secure Communication in IoT-enabled Embedded Systems for Military Applications Using Encryption," 2023 2nd International Conference on Edge Computing and Applications (ICECAA), Namakkal, India, pp. 1385–1389. Consultado el 6 de diciembre de 2023: <https://doi.org/10.1109/ICECAA58104.2023.10212400>

Khan, Saif M. and Alexander Mann. 2020. "AI Chips: What They Are and Why They Matter". Center for Security and Emerging Technology. April. Consultado el 6 de diciembre de 2023: <https://cset.georgetown.edu/publication/ai-chips-what-they-are-and-why-they-matter/>

Kharpal, Arjun. 2023. "Next-gen Mobile Internet – 6G – will Launch in 2030, Telecom Bosses Say, Even as 5G Adoption Remains Low". CNBC. 7 March. Consultado el 6 de diciembre de 2023: <https://www.cnbc.com/2023/03/08/what-is-6g-and-when-will-it-launch-telco-execs-predict.html>

Khawaja, Saleem. 2023. "How Military Uses of the IoT for Defence Applications are Expanding". Army Technology. 28 March. Consultado el 6 de diciembre de 2023: <https://www.army-technology.com/sponsored/how-military-uses-of-the-iot-for-defence-applications-are-expanding/>

Konkel, Frank. 2023. "AWS Unveils Edge Device for Defense Customers in Most Extreme Environments". Nextgov/FCW. 8 June. Consultado el 6 de diciembre de 2023: <https://www.nextgov.com/digital-government/2023/06/aws-unveils-edge-device-defense-customers-most-extreme-environments/387302/>

- Kullock, René et al. 2020. "Electrically-driven Yagi-Uda Antennas for Light". *Nature Communications* 11, 115. Consultado el 6 de diciembre de 2023: <https://doi.org/10.1038/s41467-019-14011-6>
- Kumah, Elizabeth Adjoa et al. 2023. "Human and Environmental Impacts of Nanoparticles: A Scoping Review of the Current Literature". *BMC Public Health* 23, 1059. Consultado el 6 de diciembre de 2023: <https://doi.org/10.1186/s12889-023-15958-4>
- Laursen, Lucas. 2022. "As China's Quantum-Encrypting Satellites Shrink, Their Networking Abilities Grow". *IEEE Spectrum*. 25 August. Consultado el 6 de diciembre de 2023: <https://spectrum.ieee.org/satellite-qkd-china>
- Lee, Ki et al. n.d. "Decentralized Decision Making at the Tactical Edge". Booz Allen. As of 6 January 2024: <https://www.boozallen.com/s/insight/blog/decentralized-decision-making-at-the-tactical-edge.html>
- Lee, Mary et al. 2023. "Opportunities and Risks of 5G Military Use in Europe". Santa Monica, CA: RAND Corporation. Consultado el 6 de diciembre de 2023: https://www.rand.org/pubs/research_reports/RRA1351-2.html
- Lee, Sukbae et al. 2023a. "The First Room-Temperature Ambient-Pressure Superconductor". arXiv. 22 July. Consultado el 6 de diciembre de 2023: <https://arxiv.org/abs/2307.12008>
- . 2023b. "Superconductor Pb₁₀-xCu_x(PO₄)₆O Showing Levitation at Room Temperature and Atmospheric Pressure and Mechanism". arXiv. 22 July. Consultado el 6 de diciembre de 2023: <https://arxiv.org/abs/2307.12037>
- Levine, Edlyn V. and Algirde Pipikaite. 2019. "Hardware is a Cybersecurity Risk. Here's What We Need to Know". World Economic Forum. 19 December. Consultado el 6 de diciembre de 2023: <https://www.weforum.org/agenda/2019/12/our-hardware-is-under-cyberattack-heres-how-to-make-it-safe/>
- Lewis, James Andrew. 2023. "Accelerating Federal Cloud Adoption for Modernization and Security". Center for Strategic & International Studies (CSIS). 28 July. Consultado el 6 de diciembre de 2023: <https://www.csis.org/analysis/accelerating-federal-cloud-adoption-modernization-and-security>
- Lidar, Daniel. 2023. "A Scientist Explains an Approaching Milestone Marking the Arrival of Quantum Computers". Phys.org. 20 November. Consultado el 6 de diciembre de 2023: <https://phys.org/news/2023-11-scientist-approaching-milestone-quantum.html>
- Macri, Kate. 2022. "Army is Modernizing Sensors for Data-Driven Decision-Making". GovCIO Media & Research. 4 March. Consultado el 6 de diciembre de 2023: <https://governmentciomedia.com/army-modernizing-sensors-data-driven-decision-making>

Marquina, Claudia. 2022. "How Low-Earth Orbit Satellite Technology Can Connect the Unconnected". 18 February. Consultado el 6 de diciembre de 2023: <https://www.weforum.org/agenda/2022/02/explainer-how-low-earth-orbit-satellite-technology-can-connect-the-unconnected/>

Marr, Bernard. 2023. "The 10 Biggest Cloud Computing Trends In 2024 Everyone Must Be Ready For Now". Forbes. 9 October. Consultado el 6 de diciembre de 2023: <https://www.forbes.com/sites/bernardmarr/2023/10/09/the-10-biggest-cloud-computing-trends-in-2024-everyone-must-be-ready-for-now/?sh=7ab779e66d67>

Martin, Peter et al. 2023. "Pentagon and Microsoft Are Investigating Leak of Military Emails". Bloomberg. 22 February. Consultado el 6 de diciembre de 2023: <https://www.bloomberg.com/news/articles/2023-02-22/pentagon-and-microsoft-investigating-leak-of-military-emails>

Maurer, Tim and Garrett Hinck. 2020. "Cloud Security: A Primer for Policymakers". Carnegie Endowment for International Peace. August. Consultado el 6 de diciembre de 2023: https://carnegieendowment.org/files/Maurer_Hinck_Cloud_Security-V3.pdf

Menn, Joseph. 2023. "Cyberattack Knocks Out Satellite Communications for Russian Military". *Washington Post*. 30 June. Consultado el 6 de diciembre de 2023: <https://www.washingtonpost.com/technology/2023/06/30/satellite-hacked-russian-military/>

Microsoft. 2023. "BAE Systems and Microsoft Join Forces to Equip Defence Programmes with Innovative Cloud Technology". 14 April. Consultado el 6 de diciembre de 2023: <https://news.microsoft.com/en-gb/2023/04/14/bae-systems-and-microsoft-join-forces-to-equip-defence-programmes-with-innovative-cloud-technology/>

Microsoft Azure. n.d. "What is Edge Computing?" Consultado el 6 de diciembre de 2023: <https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-edge-computing>

Miller, Kyle and Andrew Lohn. 2023. "Onboard AI: Constraints and Limitations". Center for Security and Emerging Technology (CSET). August. Consultado el 6 de enero de 2024: <https://cset.georgetown.edu/publication/onboard-ai-constraints-and-limitations/>

MIT Technology Review Insights. 2023. "Multi-die Systems Define the Future of Semiconductors". 31 March. Consultado el 6 de diciembre de 2023: <https://wp.technologyreview.com/wp-content/uploads/2023/03/Synopsys-Report-v6.pdf>

Moore, Samuel K. 2022. "3 Ways 3D Chip Tech Is Upending Computing". IEEE Spectrum. 16 March. Consultado el 6 de diciembre de 2023: <https://spectrum.ieee.org/amd-3d-stacking-intel-graphcore>

Mukherjee, Supantha. 2021. "Should We be Worried about Space Debris? Scientists Explain". World Economic Forum. 24 November. Consultado el 6 de diciembre de 2023: <https://www.weforum.org/agenda/2021/11/space-debris-satellite-international-space-station/>

National Centre of Competence in Research (NCCR). 2021. "Superconductivity, High Critical Temperature Found in 2D Semimetal Tungsten Nitride". Phys.org. 5 May. Consultado el 6 de diciembre de 2023: <https://phys.org/news/2021-05-superconductivity-high-critical-temperature-2d.html>

NATO. 2022. "Using Quantum Technologies to Make Communications Secure". 27 September. Consultado el 6 de diciembre de 2023: https://www.nato.int/cps/en/natohq/news_207634.htm

NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). 2022. "Military Movement: Risks from 5G Networks". Research Report. Consultado el 6 de diciembre de 2023: https://ccdcoe.org/uploads/2022/06/Report_Military-Movement-Risks-from-5G-Networks.pdf

Pedram, Massoud. 2023. "Room-Temperature Superconductors Could Revolutionize Electronics – An Electrical Engineer Explains the Materials' Potential". The Conversation. 28 March. Consultado el 6 de diciembre de 2023: <https://theconversation.com/room-temperature-superconductors-could-revolutionize-electronics-an-electrical-engineer-explains-the-materials-potential-201849>

Ray, Paresh et al. 2009. "Toxicity and Environmental Risks of Nanomaterials: Challenges and Future Needs". *Journal of Environmental Science and Health, Part C*, 27:1, 1–35. Consultado el 6 de diciembre de 2023: <https://doi.org/10.1080/10590500802708267>

Renals, Pete. 2021. "Future Developments in Military Cyber Operations and Their Impact on the Risk of Civilian Harm". ICRC Humanitarian Law & Policy. 24 June. Consultado el 6 de diciembre de 2023: <https://blogs.icrc.org/law-and-policy/2021/06/24/future-military-cyber-operations/>

Roa, Carlos. 2023. "Have We Created the Philosopher's Stone? Policymakers Should Care about Room-Temperature Superconductors". *National Interest*. 2 August. Consultado el 6 de diciembre de 2023: <https://nationalinterest.org/feature/have-we-created-philosopher%E2%80%99s-stone-policymakers-should-care-about-room-temperature>

Rowland, Clare E. et al. 2016. "Nanomaterial-Based Sensors for the Detection of Biological Threat Agents". *Materials Today*, 19, 8, October. Consultado el 6 de diciembre de 2023: <https://doi.org/10.1016/j.mattod.2016.02.018>

Ryugen, Hideaki. 2023. "TSMC to Make Cutting-edge 2-nm Chips at New Plant in Southern Taiwan". *Nikkei Asia*. 10 August. Consultado el 6 de diciembre de 2023: <https://asia.nikkei.com/Business/Tech/Semiconductors/TSMC-to-make-cutting-edge-2-nm-chips-at-new-plant-in-southern-Taiwan>

Samsung. 2022. "Samsung Begins Chip Production Using 3nm Process Technology with GAA Architecture". Consultado el 6 de diciembre de 2023:

<https://news.samsung.com/global/samsung-begins-chip-production-using-3nm-process-technology-with-gaa-architecture>

SpeQtral. 2022. "SpeQtral Announces SpeQtral-1 Quantum Satellite Mission for Ultra-Secure Communications". 9 February. Consultado el 6 de diciembre de 2023:

<https://speqtralquantum.com/newsroom/speqtral-announces-speqtral-1-quantum-satellite-mission-for-ultra-secure-communications>

Shilov, Anton. 2023. "The Golden Age of Custom Silicon Draws Near". EE Times. 26 July.

Consultado el 6 de diciembre de 2023: <https://www.eetimes.com/the-golden-age-of-custom-silicon-draws-near/>

Śliwa, Joanna and Marek Suchański. 2022. "Security Threats and Countermeasures in Military 5G Systems," 2022 24th International Microwave and Radar Conference (MIKON), Gdansk, Poland, pp. 1-6. Consultado el 6 de diciembre de 2023:

<https://doi.org/10.23919/MIKON54314.2022.9924818>

Taiwan Semiconductor Manufacturing Company (TSMC). n.d. "3nm Technology". Consultado el 6 de diciembre de 2023:

https://www.tsmc.com/english/dedicatedFoundry/technology/logic/l_3nm

Thomas, Arthur. 2021. "AI at the Tactical Edge for Search & Rescue Operations". Microsoft. 22 June. Consultado el 6 de diciembre de 2023: <https://www.microsoft.com/en-us/industry/blog/government/2021/06/22/ai-at-the-tactical-edge-for-search-rescue-operations/>

Tirmizi, Syed Bilal Raza et al. 2022. "Hybrid Satellite–Terrestrial Networks toward 6G: Key Technologies and Open Issues". Sensors 22, no. 21: 8544. <https://doi.org/10.3390/s22218544>

Tucker, Patrick. 2022. "How Will the Military Use 5G? A New Drone Experiment Offers Clues". Defense One. 28 September. Consultado el 6 de diciembre de 2023:

<https://www.defenseone.com/technology/2022/09/how-will-military-use-5g-new-drone-experiment-offers-clues/377745/>

UK Defence Science and Technology Laboratory. 2022. "Sensing: Defence Science and Technology Capability". 31 March. Consultado el 6 de diciembre de 2023:

<https://www.gov.uk/guidance/sensing-defence-science-and-technology-capability>

UK National Quantum Technologies Programme. n.d. "Look Around Corners with the Quantum Periscope". Consultado el 6 de diciembre de 2023: <https://uknqt.ukri.org/wp-content/uploads/2021/10/Look-Around-Corners-With-The-Quantum-Periscope.pdf>

United Nations General Assembly (UNGA). 2023. "Current Developments in Science and Technology and Their Potential Impact on International Security and Disarmament Efforts". UN document A/78/268, 1 August.

US Congressional Research Service. 2023. "Defense Primer: Quantum Technology". 25 October. Consultado el 6 de diciembre de 2023: <https://crsreports.congress.gov/product/pdf/IF/IF11836>

US Department of Defense. 2022. "Department of Defense Announces Joint Warfighting Cloud Capability Procurement". 7 December. Consultado el 6 de diciembre de 2023: <https://www.defense.gov/News/Releases/Release/Article/3239378/department-of-defense-announces-joint-warfighting-cloud-capability-procurement/>

—. 2023. "DOD Makes Headway on Cloud Computing". 29 March. Consultado el 6 de diciembre de 2023: <https://www.defense.gov/News/News-Stories/Article/Article/3345260/dod-makes-headway-on-cloud-computing/>

US National Nanotechnology Coordination Office. n.d. "What Is So Special about "Nano"?". Consultado el 6 de diciembre de 2023: <https://www.nano.gov/about-nanotechnology/what-is-so-special-about-nano>

van Amerongen, Michiel. 2021. "Quantum Technologies in Defence & Security". NATO Review. 3 June. Consultado el 6 de diciembre de 2023: <https://www.nato.int/docu/review/articles/2021/06/03/quantum-technologies-in-defence-security/index.html>

Withrington, Claire. 2023. "The Internet of Military Things". The Cove. 24 August. Consultado el 6 de diciembre de 2023: <https://cove.army.gov.au/article/internet-military-things>

Xiao, Yinhao et al. 2019. "Edge Computing Security: State of the Art and Challenges," in *Proceedings of the IEEE* 107, n8, pp. 1608–1631, August. Consultado el 6 de diciembre de 2023: <https://doi.org/10.1109/JPROC.2019.2918437>

Xu, Tammy. 2023. "Better Machine-Learning Models with Quantum Computers". IEEE Spectrum. 15 November. Consultado el 6 de diciembre de 2023: <https://spectrum.ieee.org/quantum-machine-learning-terra-quanta>