ieee.es
Instituto Español de Estudios Estratégicos

08/2019 22 de julio de 2019

*Jesús Gómez Ruedas**

Una defensa nacional para una sociedad digital

Una defensa nacional para una sociedad digital

Resumen:

Este artículo trata de mostrar una visión prospectiva de la defensa nacional hacia 2030, repasando los diferentes recursos y tecnologías de aplicación, sus casos de uso y las implicaciones de todo tipo en este campo.

Palabras clave:

Algoritmo, big data, cadena de bloques, ciberespacio, dato, defensa, digital, educación, enernet, estrategia, guerra de información, información, innovación, inteligencia artificial, logística, machine learning, realidad aumentada, realidad virtual, redes sociales, robótica, sanidad, seguridad, talento, tecnología, transformación.

A National Defence for a digital society

Abstract:

A prospective vision of the National Defence by 2030, reviewing the different resources and relevant technologies, their use cases and their global implications in this field.

Keywords:

Algorithm, big data, blockchain, Cyberspace, data, defence, digital, education, enernet, strategy, information warfare, information, innovation, artificial intelligence, Logistics, machine learning, augmented reality, virtual reality, social networks, robotics, health, security, talent, technology, transformation.

Cómo citar este documento:

GÓMEZ RUEDAS, Jesús. *Una defensa nacional para una sociedad digital.* Documento de Opinión IEEE 72/2019. enlace web IEEE y/o enlace bie[3] (consultado día/mes/año)

Introducción: hasta donde alcanza la vista

Una célebre cita del historiador británico, Thomas Carlyle, reza: «Ve hasta donde te alcance la vista; cuando llegues, serás capaz de ver más allá».

Hacia el año 1800 antes de Cristo los hicsos, pueblo semita, aparecían en Asia occidental y penetraban en Egipto de la mano de sus jinetes. Esta invasión constituiría el primer antecedente histórico del empleo del caballo como elemento de combate.

Tendrían que pasar más de treinta siglos, hasta la Segunda Guerra Mundial, para contemplar los últimos episodios bélicos protagonizados por unidades de caballería realizando sus ancestrales cargas; en todo caso, ya desde la anterior Guerra Mundial del mismo siglo, el caballo había perdido protagonismo en la primera línea de combate, quedando relegado a tareas de apoyo.

Con el paso del tiempo, el caballo, como tantas otras innovaciones en el arte de la guerra, vio relegado su rol al de un actor para representación, ocio o deporte. Sin embargo, hoy en día la tecnología ha acelerado el ciclo de la innovación. Un lapso que antes requería de miles de años, pero que hoy se ve frecuentemente reducido a unos pocos meses.

Mientras tanto, el concepto de guerra ha evolucionado hacia la defensa, la garantía de la paz y la protección de los intereses nacionales y, en definitiva, de una determinada forma de vida.

Para vislumbrar qué y cómo será la defensa nacional hacia 2030, la Estrategia de Seguridad Nacional 2017[1] proporciona una instantánea que permite caracterizar el actual entorno de seguridad global hasta donde hoy alcanza la vista: «[…] un entorno más complejo y volátil donde se observa un aumento de las tensiones geopolíticas y de la incertidumbre; un mundo cada vez más globalizado e interdependiente, donde las crisis se suceden con cada vez más intensidad. Algunas de las dinámicas más notables son el ritmo acelerado de transformación impulsado por las tecnologías, las asimetrías demográficas entre regiones o el cambio climático. Todo ello aumenta la presión sobre el orden internacional del que es partidario España, basado en la legalidad y una gobernanza global más justa, inclusiva y eficaz. El reto fundamental para España será por tanto entender, adaptarse y gestionar estos cambios de manera ágil y flexible».

[1] Gobierno de España, Presidencia del Gobierno, *Estrategia de Seguridad Nacional 2017*.

El mismo documento perfila también las actuales amenazas para la Seguridad Nacional: «Las principales amenazas identificadas son los conflictos armados, el terrorismo, el crimen organizado, la proliferación de armas de destrucción masiva, el espionaje, las ciberamenazas y las amenazas sobre las infraestructuras críticas».

La Defensa Nacional es uno de los quince ámbitos de actuación en los que se articula la respuesta a dichas amenazas.

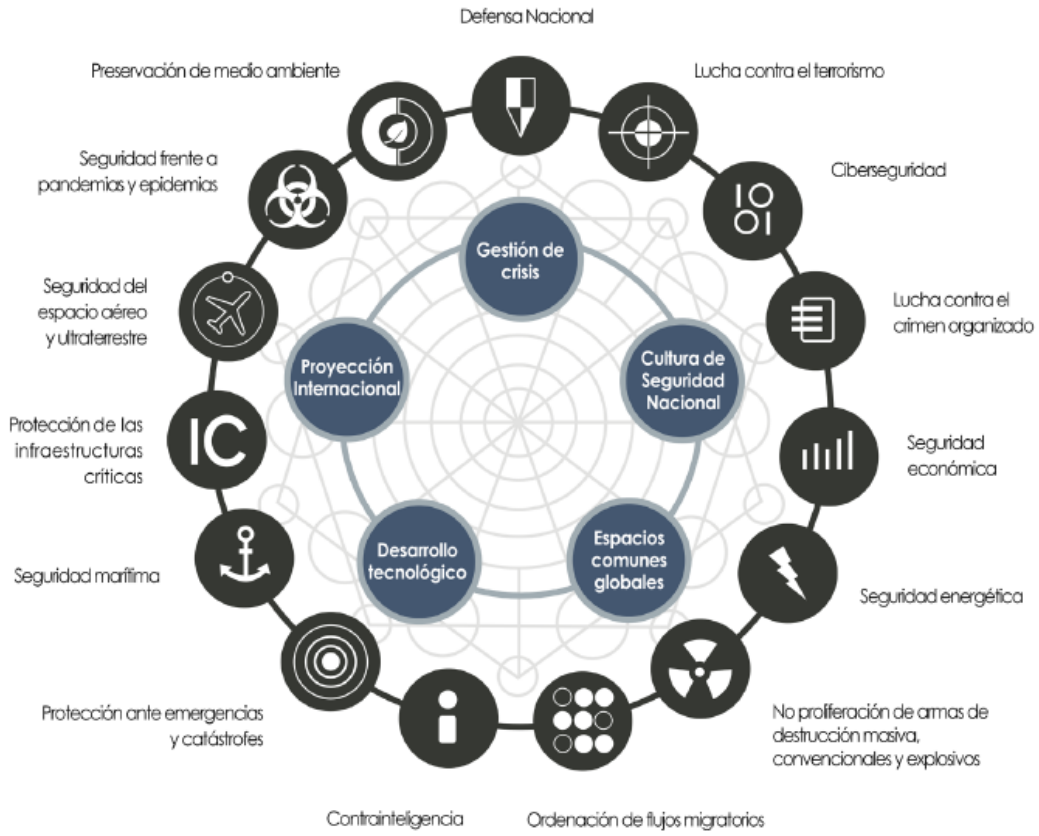

Figura 1. Objetivos generales y ámbitos de la Seguridad Nacional.
Fuente. Estrategia de Seguridad Nacional 2017.

El objetivo específico de la defensa nacional consiste en «asegurar la defensa de la soberanía e integridad de España y la protección de la población y el territorio frente a cualquier conflicto o amenaza proveniente del ámbito exterior; de forma autónoma o junto a socios y aliados. Así mismo, contribuir a crear un entorno internacional más estable y seguro mediante la proyección de estabilidad y el refuerzo de la cooperación con los socios, particularmente en las áreas de especial interés para España».

Si alguien se preguntara sobre la estabilidad de este objetivo específico parece que los únicos atributos susceptibles de cambio en dicho enunciado serían las amenazas y las áreas de especial interés para España.

Las líneas de acción para dar respuesta a este objetivo específico de la defensa nacional se fundamentan en:

1. Mejorar la capacidad de defensa autónoma con la finalidad de permitir el ejercicio de la disuasión.
2. Dotar a las Fuerzas Armadas de unas capacidades acordes con el actual escenario de seguridad y, al mismo tiempo, converger con los objetivos establecidos para la Defensa por la OTAN y el Parlamento Europeo.
3. Impulsar la estrategia industrial de defensa, para fomentar la autonomía en la adquisición de capacidades y favorecer la competitividad de la industria española.
4. Favorecer la posición de España en el sistema de seguridad internacional y, de esta forma, reforzar su liderazgo en las organizaciones internacionales.
5. Asumir un protagonismo activo dentro de la Política Común de Seguridad y Defensa de la Unión Europea, consolidando el compromiso con la OTAN y con nuevas formas de cooperación y especialización.
6. Contribuir a la instauración de un entorno regional de paz y seguridad, previniendo conflictos y conteniendo amenazas emergentes.
7. Potenciar la Diplomacia de Defensa, especialmente con países vecinos y de América Latina.

Naturalmente, ante un entorno tan complejo en el que las amenazas están conectadas, se requiere un enfoque de seguridad integral y, por supuesto, la tecnología se convierte en uno de los cinco pilares que sustentan la acción del Estado.

En la misma línea, a principios de 2018 el Ejército de Tierra daba publicidad al concepto «Brigada 2035» cuya característica principal reside en establecer la tecnología como su soporte fundamental[2]; ello debe permitirle una mayor potencia de combate con un menor número de recursos humanos.

[2] Boletín TIERRA. Brigada 2035, un nuevo concepto para futuros conflictos. 2018

El devenir del caballo como arma de guerra simboliza perfectamente una realidad histórica: las potencias mundiales de cada época han utilizado continuamente la innovación para aumentar la eficacia de sus fuerzas militares. En los tiempos modernos gran parte de esas innovaciones se relacionan con las nuevas tecnologías.

Así, en noviembre de 2014, EE. UU. ponían en marcha la Tercera Estrategia de Compensación con el fin de ampliar su ventaja en el ámbito de los sistemas de mando y control. También, durante la feria de material de la Association of the U.S. Army de 2017, un miembro del Ejército estadounidense anunciaba que en un plazo no superior a diez años dicho ejército pondría en servicio una flota de vehículos de combate totalmente eléctricos[3].

Por su parte, China desvelaba, a finales de 2015, un ambicioso programa de reforma que había sido concebido para reducir el volumen de personal militar en unos 300 000 efectivos, al mismo tiempo que se desarrollaba una modernización de la estructura de mando más idónea para la era de la Información.

Mientras tanto, la revisión de la Estrategia de Seguridad y Defensa de 2015 del Reino Unido ponía el acento en planes para fomentar su flota de vehículos no tripulados; en mejorar el equipo de las fuerzas especiales; en reclutar 1 900 especialistas de inteligencia; o en redoblar la investigación en ciberseguridad durante el siguiente lustro.

Por su parte, el Ministerio de Defensa alemán anunciaba en 2016 la creación de un mando dedicado a la información y a la ciberseguridad, integrado por 13 500 efectivos procedentes de otros servicios y organizaciones militares.

También Rusia viene desplegando de forma continuada sistemas de tecnología avanzada.

Naturalmente, toda esta vorágine de iniciativas y tecnologías emergentes repercutirá de forma notable en el futuro diseño de los ejércitos. Por supuesto, no hay que olvidar que, más allá de la tecnología, son múltiples y variados los elementos necesarios para generar cambios y producir efectos innovadores en cualquier organización. En esta línea, resulta vital la formación de alta calidad del personal y, en un sentido más amplio, la generación y retención de talento dentro de los departamentos de Defensa.

[3] Asociación para la Promoción de las Tecnologías e Industrias Estratégicas (APTIE), http://www.aptie.es/

Además, todo ello sucede en un nuevo escenario mundial caracterizado por determinados rasgos y tendencias[4]: disminuye el dominio militar de Occidente en los clásicos teatros militares (tierra, mar, aire y espacio). En particular, resurge Rusia como potencia mundial de primera línea y con una estrategia híbrida de actuación que escenifica la vieja máxima de Clausewitz, «la guerra es la actuación del Estado para conseguir objetivos estratégicos cuando no puede lograrlos con la política»; surge el ciberespacio como quinto dominio de operaciones militares en el que estados o actores no estatales, militarmente débiles, son capaces de adquirir poderosas capacidades; emerge una creciente demanda y utilización de vehículos no tripulados que apunta hacia una guerra robotizada dirigida por especialistas distantes del escenario del conflicto; esta progresiva adopción de tecnología permite vislumbrar la eliminación o reducción del componente humano en algunas de las misiones más peligrosas. En todo caso, se divisa un creciente escenario de combinación de capacidades tripuladas y no tripuladas en las futuras operaciones de las fuerzas terrestres, marítimas y aéreas; y se generaliza la extensión de las acciones armadas a las áreas urbanas.

La santabárbara[5] de la transformación digital de la Defensa

Muchas de las guerras modernas ya no se libran cuerpo a cuerpo, sino en la esfera digital. Además, las víctimas ya no se contarán solo entre las fuerzas militares o entre civiles atrapados en una zona determinada del conflicto; ahora cualquier ciudadano de a pie puede ser atacado a través de sus dispositivos personales en forma de noticias falsas, desinformación y otras técnicas de manipulación, persuasión y ocultación que consiguen desestabilizar procesos electorales y amenazan el propio modelo occidental de vida y gobierno.

Ciertamente, más allá de las diferentes vertientes que ofrece el universo Internet (rentabilidad empresarial, desarrollo social, derecho humano, herramienta para reducir desigualdades, espacio para la creatividad y las oportunidades, etc.), quien maneja información y datos de forma intensiva, eficaz y eficiente dispone de una nueva arma.

[4] ARGUMOSA, Jesús. *Tendencias que afectarán a las Fuerzas Armadas 2050*. Documento de Opinión IEEE 117/2017. Disponible en: http://www.ieee.es/contenido/noticias/2017/11/DIEEEO117-2017.html

[5] Santabárbara: Pañol o paraje destinado en las embarcaciones para custodiar la pólvora.

Figura 2. Big Data. Fuente. Big Data Spain.

Datos y machine learning

A la hora de la toma de decisiones, la intuición humana es un recurso casi prohibido en las empresas más valiosas y competitivas del mundo. Cualquier acción a ejecutar debe sustentarse en datos. También en el ámbito de la defensa los datos ayudan a entender el desempeño de los procesos operativos, cuándo hay una mejora en la eficacia o el rendimiento de un sistema de armas, cómo integrar e interpretar los datos procedentes de los sensores de inteligencia, cómo disponer del personal mejor adiestrado, cómo planificar las operaciones, cómo simplificar la logística, etc.

Pero, en cualquier caso, el valor de los datos no es obvio ni inmediato. Lo que crea valor es la adecuada explotación y la gestión de los datos.

Indudablemente, las tecnologías de big data[6] y *machine learning* formarán parte del ADN de la defensa para los próximos lustros. Las herramientas analíticas y el aprendizaje automático formarán parte de sus procesos y de sus actividades rutinarias. En la búsqueda de la conocida «Superioridad de la Información»[7] tomarán la delantera

[6] *Big data* es el anglicismo que alude al almacenamiento y la gestión de una cantidad elevada de datos

[7] Superioridad de la Información: Ventaja relativa que se genera mediante el empleo de información relevante, principios y capacidades disponibles, de forma continua y dirigida, adaptándose a cada

aquellos Ejércitos capaces de obtener y mantener los algoritmos más potentes; y dichos algoritmos necesitarán de datos con los que ser alimentados. En consecuencia, resultará imprescindible orientar cada proceso de negocio a los datos que maneje: habrá que definir los objetivos, preparar y transformar los datos, construir y evaluar modelos, realizar predicciones, etc.

Machine learning es, en esencia, un conjunto de herramientas que permiten que una máquina aprenda de unos datos de forma iterativa. De esta manera, será capaz de desarrollar modelos de forma automatizada, con la particularidad de que dichos modelos no han sido específicamente programados por una persona. Esta herramienta posee suficiente capacidad de disrupción respecto a la forma en que se vienen haciendo las cosas como para convertirse en una clara ventaja competitiva. Dado que los algoritmos que se desarrollan se adaptan a los datos y terminan por generar mejores predicciones y resultados que los desarrollados por personas, la organización que utilice *machine learning* obtendrá una mayor eficiencia, mejores prestaciones, más agilidad o funciones que antes podían resultar imposibles de obtener[8].

Pero como herramienta, el *machine learning* no es algo que se pueda «comprar e instalar», porque depende de los datos, de su calidad y de su accesibilidad; y requiere por ello de una completa orientación al dato, una «data-centricidad». Solo aquellas compañías que sean capaces de orientarse a la generación y proceso de datos estarán en condiciones de recoger los frutos del *machine learning* y convertirlos en verdaderas ventajas competitivas. Aquellos departamentos de Defensa que consigan obtener y mantener algoritmos más inteligentes y potentes adquirirán una clara posición de ventaja en todos sus procesos y actividades de negocio. Para ello, necesitarán disponer de datos con los cuales alimentar dichos algoritmos que, a medida que son alimentados con nuevos datos, van incrementando sus capacidades de análisis de datos y, en consecuencia, son capaces de generar predicciones, o de detectar excepciones, de aislar patrones o de afrontar situaciones hipotéticas no probadas anteriormente. Así, por ejemplo, cada vehículo autónomo operando en contextos y escenarios diferentes alimenta un único algoritmo común, multiplicando su rendimiento y eficiencia y, por tanto,

situación. Este concepto debe entenderse más como la capacidad de adaptación al entorno cambiante en el que se actúe, que como el control de la información en sí misma

[8] DANS, Enrique. Blog disponible en: https://www.enriquedans.com

exprimiendo cada proceso y actividad hasta límites insospechados. Los datos son el combustible de las organizaciones modernas.

En consecuencia, el primer paso que tendrán que afrontar las organizaciones responsables de la defensa nacional es orientarse hacia la generación, organización, análisis y explotación de los datos. De este modo, posteriormente, los sistemas de inteligencia artificial podrán generar alertas, respuestas y soluciones de negocio, ya sea en ámbitos operativos, de gestión de recursos o de cualquier otra área de los productos y servicios del ámbito de la Defensa.

Probablemente, el triunvirato big data, *machine learning* e Inteligencia Artificial asumirá el protagonismo estelar de la próxima revolución de las Tecnologías de la Información. Como señalaba hace algunos meses el CEO de Google, su impacto en la historia de la humanidad será comparable al de la electricidad o el fuego. Pero antes de continuar recorriendo la senda de la generación y tratamiento de los datos conviene detenerse en otro recurso clave del «arsenal digital».

Capital humano digital

Como se ha señalado, tarea crucial para ese empoderamiento del dato es su preparación. Surge aquí uno de los nuevos perfiles profesionales necesarios en este nuevo universo, el científico de datos, pero no será ésta la única habilidad necesaria. Y es que las personas constituyen el principal activo de cualquier organización que aspire a completar y consolidar con éxito un verdadero proceso de transformación digital. Si la cultura digital de sus empleados y directivos no alcanza un determinado nivel, proporcional a sus responsabilidades, será imposible «cruzar el Rubicón» de la citada metamorfosis. Este requisito emerge con la misma criticidad en la Administración de Defensa, pues es imprescindible atraer y retener talento con el necesario nivel de cultura digital.

En la sociedad actual, ninguna organización puede asumir que un empleado carezca de un determinado nivel de alfabetización digital. No solo sería un problema de actitud del empleado, sino, sobre todo, un problema de capacidad de la propia organización. Evidentemente, tal vulnerabilidad resultaría especialmente grave y peligrosa en caso de arraigar en los estratos medios y altos de la dirección de la organización. Los máximos

responsables de la toma de decisiones y de la gestión de la información corporativa deben acreditar un apreciable nivel de cultura y competencia digital.

Figura 3. Capital humano. Fuente. Ejército de Tierra.

Un reciente estudio desarrollado por el Instituto Tecnológico de Massachusetts viene a demostrar que las noticias falsas se difunden hasta veinte veces más rápido en Twitter que las verdaderas; la culpa no recae sobre los bots[9], sino sobre las personas. La educación constituye el elemento fundamental ante problemas de este tipo. Solo una adecuada formación desde los escalones básicos del sistema educativo nacional permitirá sobrevivir entre la marabunta de datos de la era de la información. Es imprescindible capacitar a todos los miembros de cualquier organización para desarrollar mecanismos adecuados de búsqueda y cualificación de la información; es una habilidad fundamental en un entorno social caracterizado por la hiperabundancia y la saturación de información.

La corta historia de las redes sociales ilustra sobradamente esta vulnerabilidad que caracteriza a amplios sectores de la sociedad; y es que lejos de cubrir completamente su expectativa como herramientas de difusión de información y de fortalecimiento de las

[9] *Bot* es una máquina o ingenio electrónico programable, capaz de manipular objetos y realizar operaciones antes reservadas solo a las personas

libertades, dichas redes se han convertido en fuentes de desinformación, haciendo del ciberespacio un factor de desestabilización[10] donde la distinción entre lo real y lo falso no siempre resulta trivial.

En su momento, en los primeros compases del siglo XXI, muchos expertos de diversas disciplinas creyeron ver en el potencial de Internet una herramienta para reordenar ciertos escenarios ajenos al modelo democrático de Occidente sin necesidad de desplegar ejércitos. Al hilo de lo anterior, no pocos países, cuyo patrón de gobierno no coincide con el citado modelo de democracia, comenzaron a percibir las redes sociales y otras aplicaciones del ciberespacio como vectores de desestabilización urdidos o potenciados por potencias extranjeras. Como respuesta, empezaron a desarrollar capacidades para detectar y contrarrestar cualquier información que pudiera suponer algún tipo de amenaza o, en otros casos, entenderse como desinformación o propaganda contraria a los correspondientes regímenes. Pero en el otro dominio, supuestamente libre y democrático, también se vienen suscitando dudas acerca de la capacidad de manipulación de ciertas esferas políticas, económicas y sociales. ¿Y si el verdadero problema no fuera únicamente la censura, sino, además, el eventual proceso de desinformación orientado a manipular el pensamiento y las acciones de amplios sectores de la población? ¿Supondría este proceso un peligro para la estabilidad de la sociedad debido a la falta de filtros a la hora de publicar información?

Las redes sociales pueden favorecer unas sociedades más plurales, pero ese pluralismo, imprevisible e inestable, puede afectar a la seguridad global al ser utilizado como arma en contra de los adversarios. Este escenario puede desencadenar una militarización de las redes sociales.

Para responder a estas amenazas las nuevas generaciones han de adquirir una formación que les permita gestionar el peligro de manipulación subyacente en las redes sociales, desarrollar un juicio crítico y, en consecuencia, evitar caer en las redes del proceso de desinformación. Como señala el profesor Dans[11], ello permitirá transitar desde la «era de la información», basada en el acceso a la mayor cantidad de información posible, a la «era de la reputación», caracterizada por la capacidad de

[10] CARLINI, Agnese. *Las redes sociales como factor de desestabilización*. Documento de Opinión IEEE 79/ 2018. Disponible en: http://www.ieee.es/contenido/noticias/2018/07/DIEEEEO79-2018.html

[11] DANS, Enrique. Blog disponible en: https://www.enriquedans.com

discernir la calidad y fiabilidad de la información. Es crítico eliminar cuanto antes la nueva categoría de «pobre contemporáneo», aquella persona que sistemáticamente acepta como verdad absoluta cualquier noticia que aparece en la pantalla y que es incapaz de diferenciar una fuente fiable de una que no lo es. La información tiene valor si está verificada, filtrada y evaluada. De este modo, la reputación se convierte en pieza fundamental del proceso de construcción de inteligencia colectiva.

Otra pregunta que deja en el aire este proceso de transformación es el futuro reparto de tareas entre hombres y máquinas: ¿Se limitará a la mera sustitución de los trabajos enmarcados en la categoría 4D, *Dull* (aburridos), *Demeaning* (degradantes), *Dirty* (sucios) y *Dangerous* (peligrosos) o el alcance será sensiblemente mayor?, ¿qué tipo de sociedad cabe imaginar a medida que las máquinas vayan asumiendo un mayor número de tareas? Indudablemente, en las Fuerzas Armadas abundan las actividades de naturaleza peligrosa, así como otras muchas de carácter repetitivo enmarcadas en los procesos logísticos de movimiento de recursos materiales. Por supuesto, aquí se abre un amplísimo campo de acción para desarrollar proyectos que permitan sustituir por máquinas los recursos humanos dedicados a tales tareas para, a continuación, reorientarlos hacia otras actividades donde puedan generar mayor valor para la organización.

Inteligencia Artificial

Las tecnologías relacionadas con el tratamiento intensivo de grandes volúmenes de datos y con el aprendizaje de las máquinas se encuentran en la base de la que se considera la mayor disrupción de los próximos años: la Inteligencia Artificial.

Los analistas de Gartner[12] estiman que su potencial permitirá a las organizaciones adaptarse a nuevas situaciones y solucionar problemas a los que nadie se había enfrentado anteriormente. En consecuencia, recomiendan a las organizaciones que quieran destacar en este campo que presten especial atención a las siguientes tecnologías: aprendizaje profundo, inteligencia artificial general, vehículos autónomos, computación cognitiva, drones comerciales, interfaces de conversación con usuarios,

[12] Gartner Inc. Gartner says by 2020, Artificial Intelligence will create more jobs than it eliminates. 2017

gestión de ontología y taxonomía empresarial, *machine learning*, *smart dust*[13], robots inteligentes y trabajo inteligente.

Según una encuesta desarrollada por el MIT, el 85 % de los directivos considera la Inteligencia Artificial como una tecnología importante que permitirá a sus compañías entrar en nuevos negocios y obtener ventajas competitivas. En cambio, menos del 39 % de esas organizaciones tiene algún tipo de estrategia respecto a Inteligencia Artificial. Y en el ámbito público, ¿cuántos gobiernos nacionales están desarrollando un plan estratégico para impulsar la Inteligencia Artificial? El presidente francés ya ha anunciado sus planes tomando la sanidad y el transporte como epicentro del proyecto. Por otro lado, China se presenta claramente lanzada a la conquista de la hegemonía mundial en este conjunto de tecnologías. Más recientemente, el presidente ruso ha dado instrucciones a su gobierno para que cree una estrategia nacional de investigación y desarrollo de Inteligencia Artificial. Por supuesto, las grandes multinacionales norteamericanas llevan tiempo trabajando en ello y, paralelamente, atrayendo todo el talento de muchos países aparentemente desinteresados en esta revolución tecnológica, económica y social.

No cabe duda de que la Inteligencia Artificial va a eclipsar a la conocida Ley de Moore[14] como vehículo de innovación. La sociedad asiste a una verdadera carrera para replantearse cómo se harán muchas cosas en el futuro mediante la Inteligencia Artificial; cómo se puede incorporar a los productos y servicios existentes; cómo integrarla para evitar quedar rezagado frente a los que consigan hacerlo. De cualquier forma, la carrera ya ha empezado y muchas organizaciones siguen en la línea de salida.

Pero precisamente del ámbito armamentístico proceden las principales preocupaciones respecto al desarrollo de estas tecnologías. Más de cien expertos en robótica e Inteligencia Artificial han dado la voz de alarma y han pedido en una carta abierta dirigida a la ONU que se prohíba la creación de robots soldado y de armas autónomas letales[15]. Recalcan que es imprescindible una regulación del uso de la Inteligencia Artificial antes de que sea demasiado tarde y temen que, de no ser así, estas tecnologías puedan

[13] *Smart dust* es el polvo inteligente es una red inalámbrica de minúsculos sensores microelectromecánicos, robots o dispositivos que pueden detectar señales de luz, temperatura, vibraciones, etc.

[14] La Ley de Moore expresa que aproximadamente cada dos años se duplica el número de transistores de un microprocesador.

[15] Disponible en: https://futureoflife.org/autonomous-weapons-open-letter-2017

utilizarse para operar ejércitos de robots que posibilitarán el control masivo de la población o el enmascaramiento de actividades humanas no éticas.

También en el sector privado algunas compañías, como Google[16], han publicado su declaración de principios respecto a la IA.

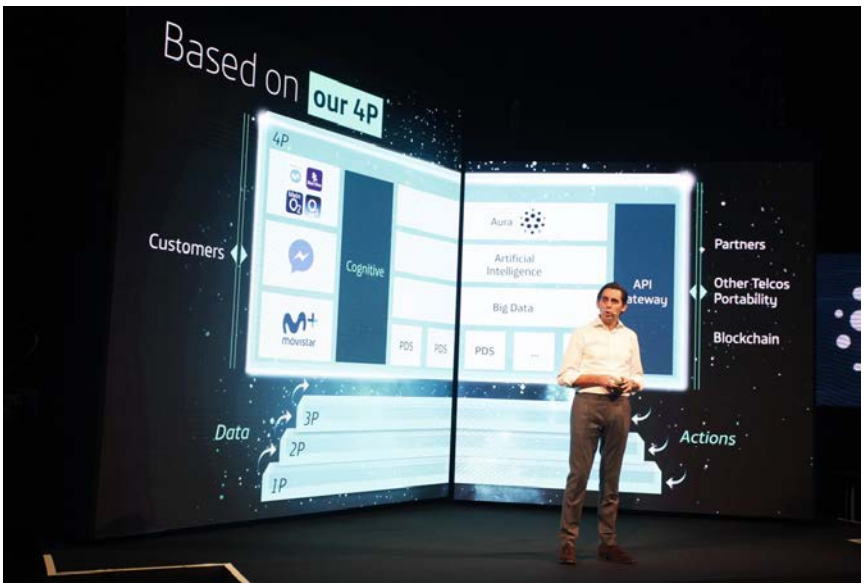

Figura 4. Inteligencia Artificial. Fuente. Telefónica.

En todo caso, no cabe duda de que la IA va a condicionar de forma clave la evolución de la sociedad y su capacidad de generación de riqueza. Urge, por tanto, avanzar en el análisis de su estrategia y su modelo de gestión. Condicionará la vida de los ciudadanos y temas tan sensibles como sus derechos, libertades y, en definitiva, su modo de vida en una nueva sociedad en la que las máquinas, gracias a potentes esquemas de aprendizaje, realizarán cada vez más tareas y con una eficiencia superior a la del hombre.

[16] AI at Google: our principles, Jun 2018.

Realidad virtual[17] y realidad aumentada[18]

Otra característica de algunas de las tecnologías incipientes es que, poco a poco, estarán más focalizadas en las personas, de forma que llegarán a ser más transparentes, tendencia que se ha de acelerar a medida que se adapten a todas las facetas de la vida humana. En esta orientación se encuentran la impresión 4D, la realidad aumentada, los interfaces ordenador-cerebro, el hogar conectado, la realidad virtual o los displays volumétricos.

En particular, en el marco de actuación propio de las Fuerzas Armadas adquirirán gran relevancia la realidad virtual y la realidad aumentada. Ambas ofrecerán multitud de escenarios que enriquecerán todo tipo de actividades, desde trabajos independizados de lugar y tiempo, hasta posibilidades de todo tipo aplicadas al aprendizaje.

Mientras la realidad virtual ofrece grandes expectativas en la simulación de escenarios para el adiestramiento militar y la preparación de operaciones, la realidad aumentada presenta un amplio abanico de usos prácticos, más cercanos a las actividades ordinarias, para configurar un ecosistema cada vez más potente. En definitiva, la realidad aumentada constituye una nueva interfaz de usuarios para un número incremental de aplicaciones y suficientemente maduro para convertirse en una parte integrante de la vida cotidiana.

Más allá de la simple proyección a corta distancia de los ojos de una serie de imágenes que permiten la creación de un entorno inmersivo o de una capa superpuesta sobre la realidad, la realidad aumentada posibilita la redefinición de una buena parte del trabajo diario, como, por ejemplo, la capacidad de interaccionar con la información, el aprendizaje y una amplísima variedad de tareas más. Se trata de una tecnología que trasladará su impacto a una gran cantidad de actividades y se convertirá en prácticamente ubicua.

[17] La realidad virtual es un entorno de escenas u objetos de apariencia real. La acepción más común refiere a un entorno generado mediante tecnología informática, que crea en el usuario la sensación de estar inmerso en él.

[18] La realidad aumentada es el término que se usa para definir la visión de un entorno físico del mundo real, a través de un dispositivo tecnológico. Este dispositivo o conjunto de dispositivos, añaden información virtual a la información física ya existente; es decir, una parte sintética virtual solapada a la real.

Por su parte, la realidad virtual inmersiva, que encuentra sus orígenes fundamentalmente en el mundo de los videojuegos, generó inicialmente una atención mucho mayor que la realidad aumentada. Actualmente, en cambio, todo indica que será esta última la que, en el futuro, atraerá una mayor atención y un mayor número de aplicaciones prácticas en un plazo razonablemente cercano.

***Enernet*[19]**

A principios de 2018, el primer ministro del gobierno del sur de Australia anunciaba un acuerdo con la empresa *Tesla* para dotar de techos solares y baterías acumuladoras a 50 000 hogares de dicha región con la finalidad de crear la mayor central eléctrica virtual del mundo. Será el primer gran proyecto de aplicación del concepto «Enernet». El proyecto se basa en instalar en los hogares de forma gratuita los paneles solares y las baterías *Powerwall* de *Tesla* a cambio de la cesión de la energía generada y su venta a los usuarios a precios ventajosos, con el correspondiente ahorro en sus facturas. El resultado final equivaldrá a la construcción de una central eléctrica de 250 megavatios, con una capacidad de almacenamiento de 650 megavatios.

En definitiva, Enernet significa la aplicación del modelo en red de Internet a la generación de energía eléctrica, aprovechando la disponibilidad de la fuente de energía más inagotable, el sol. Lógicamente, la ciudadanía interconectada podrá equilibrar esa energía en función de sus niveles de producción y de gasto. Dicha interacción podrá realizarse por medio de transacciones basadas en tecnología *blockchain*.

Desde el punto de vista de las Fuerzas Armadas, este modelo de generación de energía distribuida en un escenario en el que irá aumentando progresivamente el número de vehículos y dispositivos alimentados con energía eléctrica, con fuerzas desplegadas o con instalaciones críticas como hospitales de campaña, aeródromos o centros de mando y control de diversa naturaleza, presenta prometedoras expectativas.

De la misma forma que, en su momento, Internet o la computación distribuida supusieron un alto impacto, es de esperar que Enernet, más allá de las implicaciones

[19] La palabra Enernet se encuentra compuesta por dos vocablos: energía y red. Se configura como una red de energía dinámica, construida alrededor de la generación, acumulación y entrega de energía limpia, que considera la aplicación del modelo de internet a la producción de energía eléctrica y que se basa en los avances tecnológicos.

medioambientales, conlleve cambios significativos en la planificación y empleo de muchos recursos y operaciones del Ministerio de Defensa.

Blockchain

No se puede dejar de citar esta tecnología emergente llamada a revolucionar la práctica totalidad de los procesos de negocio introduciendo cambios radicales en la forma de acceder a los datos y en las capacidades de proceso. Innovaciones que, por supuesto, también afectarán a los procesos de la defensa[20] como, por ejemplo, el control de las cadenas de suministro, los mecanismos de ciberseguridad o la activación de sistemas de armamento.

Blockchain es la esencia de la transaccionalidad. Todo aquello que pueda ser definido como una transacción, sea un intercambio económico o de otro tipo, tendrá como base una cadena de bloques, una solución elegante e imaginativa diseñada para garantizar su integridad. La adopción de *blockchain* en todos los sectores de la sociedad determinará una fortísima ganancia de agilidad y el cambio en el funcionamiento de muchos mecanismos. Su impacto se verá en todas partes, incluyendo nuevas alternativas para otras tecnologías conocidas, como se ha señalado en el caso de Enernet.

Blockchain (literalmente, cadena de bloques) es una tecnología que forma parte de las denominadas tecnologías de registro distribuido (DLT, por sus siglas en inglés). Permite gestionar datos, órdenes, transacciones, activos y *tokens*[21], mediante un sistema de registro distribuido o descentralizado que se anota en bloques de información, los cuales se encadenan secuencialmente creando una cadena de bloques o registros inmutable e inalterable, compartida colaborativamente entre todos los miembros de cada red de *blockchain*, y que son verificados por dichos miembros de la red, actuando como nodos de la misma. De esta forma, se crea un procedimiento de registro, que funciona mediante

[20] PALOMO-ZURDO, Ricardo. *Blockchain: la descentralización del poder y su aplicación en la defensa*. Documento de Opinión IEEE 70/2018. Disponible en: http://www.ieee.es/contenido/noticias/2018/07/DIEEEEO79-2018.html

[21] *Token* es un mecanismo que se le da a un usuario autorizado de un servicio informático para facilitar el proceso de autenticación.

criptografía, en modo equivalente a un libro contable digital del que hay tantas copias idénticas como miembros de la red.

Por tanto, mediante *blockchain* se puede crear una base de datos distribuida, descentralizada, compartida y replicada, que puede ser pública o privada, permisionada (accesible solo a quienes son admitidos como miembros de la red) o no permisionada (de acceso libre para cualquier usuario que desee hacerlo mediante la instalación del software libre apropiado).

Blockchain es conocido como el «Internet del valor» o el «Internet de la confianza», frente al actual «Internet de la información», dado que permite transferir valor o activos digitalizados entre los usuarios, frente al actual Internet que solo permite enviar información o copias de activos. En definitiva, la propia red actúa como fedatario introduciendo sistemas de confianza entre desconocidos, ya que usuarios que no confían plenamente unos en otros deben mantener un consenso sobre la existencia, el estado y la evolución de una serie de factores compartidos.

Una de las redes *blockchain* permisionadas a nivel nacional es Alastria[22] compuesta por más de 200 miembros. Desgraciadamente, en septiembre de 2018, la presencia del sector público se limitaba a unas pocas empresas públicas. Sin duda, sería positivo que la Administración General del Estado subiera a esta ola de innovación que, con toda seguridad, tendrá implicaciones para el marco legislativo de la sociedad digital que, lógicamente, afectarán a todos los sectores de la Cuarta Revolución Industrial.

Figura 5. Tecnología *blockchain.* Fuente. Cryptoconsulting.info.

[22] Disponible en: https://alastria.io

Precisamente su naturaleza de sistema distribuido, en contraposición a los habituales modelos centralizados, es lo que impulsará el cambio de muchos modelos de negocio, marcos de gestión y de organización institucional. En el ámbito de la Defensa las iniciativas de aplicación son múltiples:

- ✓ Control de la integridad de los componentes de las cadenas de suministro que proveen los sistemas de defensa.
- ✓ Detección y protección frente a amenazas diseñadas para permanecer ocultas en las redes (proyecto ya emprendido por la agencia norteamericana DARPA[23]).
- ✓ Logística, adquisiciones e Internet de las Cosas (proyectos en fase inicial por parte de la Agencia NCIA[24] de la OTAN).
- ✓ Desarrollo de sistemas de mensajería militar que sean seguros y no hackeables.

En todo caso, no hay que olvidar que, a pesar de su interés y prometedor futuro, las tecnologías de cadena de bloques todavía deben sortear algunos riesgos y vencer algunas desconfianzas, por lo que requerirán un dilatado periodo de maduración hasta que superen la fase de experimentación y se generalice su implantación.

Así será la Defensa después de la transformación digital

En 2013, el entonces jefe del Estado Mayor de las Fuerzas Armadas de Rusia, el general Valery Gerasimov, publicó el artículo *El valor de la ciencia está en la previsión* donde se exponía una nueva táctica que se ha convertido en la moderna arma de la guerra contemporánea: hackear[25] al enemigo para generar un ambiente de permanente inquietud y conflicto. Así nacía la «propaganda 2.0».

Por su parte, Lisa-Maria Neudert, investigadora del Oxford Internet Institute, señalaba[26] que la novedad no es la propaganda en sí como herramienta de manipulación, sino que la diferencia con el siglo pasado radica en lo sencillo, rápido, global y barato que resulta crear una campaña que incline la balanza hacia uno u otro lado. Los hábitos en Internet

[23] DARPA: *Defense Advanced Research Projects Agency* (Agencia de Proyectos e Investigación Avanzados de Defensa).

[24] NCIA: *NATO Communications and Information Agency* (Agencia de Información y Comunicaciones de la OTAN).

[25] Hackear consiste en acceder sin autorización a computadoras, redes o sistemas informáticos, o a sus datos.

[26] Disponible en: https://comprop.oii.ox.ac.uk/the-team/research/lisa-maria-neudert/

se han convertido en la nueva munición de la guerra digital. Como una de las consecuencias de esta guerra surge el término «posverdad»[27] como distorsión deliberada de la realidad, manipulando creencias y emociones con el fin de influir en la opinión pública y las actitudes sociales de la población objetivo. Los investigadores estiman que una noticia ficticia se disemina a 1 500 usuarios en 10 horas, mientras que una historia contrastada tarda unas 60 horas en alcanzar al mismo número de personas. Se trata de una nueva arma que ya han empezado a utilizar todo tipo de organizaciones, tanto privadas como estatales; se trata de la guerra digital.

Por lo tanto, los responsables de la defensa nacional deben conocer el alcance del problema y, de este modo, estar en condiciones de prevenirlo o, en su caso, de resolverlo. Para ello, los mencionados escalones directivos necesitan orientar la actividad de los procesos de Defensa hacia la generación de datos analizables y, seguidamente, asimilar qué tareas pueden realizar los algoritmos.

La guerra de la desinformación

El concepto de «Guerra de información»[28], surgido a finales del siglo XX, engloba numerosos aspectos propagandísticos y de guerra psicológica encaminados a debilitar y derrotar al enemigo sin necesidad de un enfrentamiento físico. No obstante, la guerra de información se diferencia tanto de la propaganda como de la guerra psicológica por los tiempos en los que se ejecuta y por los destinatarios que tiene esta última; mientras que la propaganda intenta convencer a una audiencia de una determinada idea, la guerra informativa va mucho más lejos, al intentar mermar las capacidades defensivas y ofensivas del enemigo, debilitando la competencia de sus élites para tomar decisiones. Por su parte, la guerra psicológica va encaminada a atacar y adulterar las percepciones cognitivas de las fuerzas armadas y de la población enemiga en tiempos de guerra, mientras que en la guerra de información este fenómeno puede producirse también en tiempo de paz.

---

[27] MARTÍNEZ DÍAZ, Gonzalo. *La posverdad y el resquebrajamiento del orden liberal*. Documento de Opinión IEEE 93/2018 Disponible en: http://www.ieee.es/publicaciones-new/documentos-de-opinion/2018/DIEEEO93-2018Posverdad.html

[28] MORENO MERCADO, José Manuel. *Evolución histórica de la gestión de la información en conflictos bélicos.* Documento Marco 18/2017. Disponible en: http://www.ieee.es/contenido/noticias/2017/11/DIEEEM18-2017.html

La guerra de información se caracteriza por tres rasgos específicos: se ejecuta a través de los medios de difusión masiva de información; se dirige a combatientes y no combatientes; y se enfoca a enemigos internos y externos. Por lo tanto, el concepto engloba prácticamente todos los aspectos relativos a la recogida, análisis, procesamiento y gestión de la información, siendo esta última una variable crucial tanto en el desarrollo de acciones bélicas como en operaciones de debilitamiento de carácter político.

Actualmente, dentro de un contexto de situación de paz, en algunos países ajenos al modelo democrático occidental, el gobierno dedica más personas a la eliminación y manipulación de contenidos en las redes sociales que a otras fuerzas convencionales de su ejército, es decir, una parte significativa de la población se dedica, en su día a día, al trabajo, digno del Ministerio de la Verdad de Orwell[29], de fabricar una realidad alternativa para el resto de sus conciudadanos, eliminando toda participación anónima, crítica o considerada no aceptable, e insertando opiniones laudatorias hacia el gobierno en foros, redes y periódicos utilizando múltiples cuentas para simular un apoyo masivo. No es el único caso de régimen político en el que miles de trolls[30], bots y cuentas falsas dedican su día a día a proteger el liderazgo del máximo mandatario de la nación y a manipular el panorama político a su favor. Para estos fines utilizan un conjunto de herramientas y técnicas de automatización de la desinformación.

Lógicamente, estas herramientas que, por ejemplo, hoy se utilizan de manera organizada y siguiendo estrategias definidas para manipular y generar estados de opinión en procesos electorales de otros países, están disponibles y en proceso de continuo aprendizaje y mejora para ser empleadas en una situación de confrontación militar, tanto dirigidas a la población propia como a la del país en conflicto. La combinación de las técnicas de manipulación de imágenes, de audios y de cualquier pieza de información, unido a la referida potencia multiplicadora de las noticias falsas conforma un auténtico coctel idóneo para la guerra de la información. Esta moderna arma digital ya se viene utilizando a diario en múltiples escenarios, como el conflicto de Oriente Próximo y, como ya se ha señalado, será necesario un importante esfuerzo en el nivel educativo de la población para combatir sus efectos. En el aire queda la duda de si todos los gobernantes

[29] ORWELL, George. *1984*.

[30] *Troll* es una persona que publica en internet mensajes provocadores, irrelevantes o fuera de lugar, con la intención de molestar o provocar una respuesta emocional negativa en los usuarios y lectores.

están convencidos en cualquier circunstancia de las bondades y beneficios de contar con una población altamente cualificada desde el punto de vista digital y capaz de razonar y analizar de una forma objetiva cual es el grado de verdad de lo que se publica a cada instante en los medios digitales.

La logística militar

Sin duda, multitud de actividades en el universo de la logística militar cambiarán de forma significativa en los próximos lustros.

En primer lugar, los almacenes parecen el escenario idóneo para que algunos de los trabajos pertenecientes a la categoría 4D contemplen la sustitución de trabajadores humanos por robots en no pocas tareas aburridas, sucias o peligrosas.

Tanto en los almacenes y parques situados en territorio nacional como en aquellos otros proyectados en zonas de operaciones, así como en las tareas de abastecimiento y suministro entre los diferentes centros logísticos, se impondrán pautas y protocolos focalizados en la eficiencia y en la automatización, con la finalidad mejorar la velocidad de respuesta, eliminar la tasa de errores e incidencias y, además, disponer de una mayor trazabilidad del proceso de provisión de recursos. En este contexto, los vehículos de conducción autónoma adquirirán un protagonismo relevante en los almacenes antes de dar el salto a la vía pública. Evidentemente, este proceso de innovación tendrá, entre otras, varias consecuencias interesantes: por un lado, la eficiencia de la cadena logística implicará un incremento en el grado de operatividad y disponibilidad de las fuerzas militares; por otra parte, la reducción de personal dedicado a tareas manuales permitirá su asignación a otras actividades y puestos con mayor valor para la operatividad de las unidades militares; a la postre, constituirá un soporte fundamental para la mejora de los procesos corporativos de gestión de activos.

Naturalmente, en el último tramo de la cadena logística, el del suministro directo a las fuerzas desplegadas, el reparto aéreo a través de drones se convertirá en práctica habitual.

Por otra parte, se atisba que la flota de vehículos protagonizará numerosos cambios. De un lado, como ya se ha comentado en relación al ejército estadounidense, se generalizará el empleo de vehículos eléctricos. Además, este proceso se relacionará con los nuevos métodos de generación y distribución de energía, como la citada Enernet.

Además, se incrementará el nivel de monitorización de los vehículos de combate, de modo que, por ejemplo, se pueda desencadenar el aviso inmediato a los servicios de emergencia en caso de accidente u otro tipo de incidencia o bien, en otros casos, puedan recibir indicaciones sobre circunstancias especiales o restricciones de movimiento. A modo de ejemplo, en Dubai ya se está realizando una experiencia piloto de vehículos con matrículas inteligentes que centralizan la gestión de la sensorización del vehículo[31].

Finalmente, este paradigma de vehículos monitorizados permitirá incrementar el nivel de automatización de los sistemas logísticos y, por tanto, la agilidad y velocidad de respuesta de la cadena de provisión de recursos.

Por supuesto, no hay que olvidar que todos estos procesos de robotización de actividades logísticas estarán controlados y supervisados por humanos, de forma que, tras un periodo inicial de adaptación al nuevo entorno y operativa, los robots serán percibidos como valiosos colaboradores para tareas más o menos ingratas, antes que como una amenaza que sustituyen a las personas.

Robótica y plataformas autónomas para el combate

A pesar de las referidas, y prudentes, reticencias de más de un centenar de expertos en Inteligencia Artificial acerca de la aplicación de estas tecnologías a la robotización y las armas autónomas letales, no cabe duda de que los ambientes operativos militares están repletos de actividades peligrosas. Parece lógica la introducción de robots para la realización de buena parte de dichas actividades.

Además de reforzar y mejorar los actuales mecanismos internacionales de control de la fabricación y transferencia de armamentos, resulta conveniente que los organismos multinacionales promuevan salvaguardas que garanticen que las plataformas autónomas

[31] DANS, Enrique. Blog disponible en: https://www.enriquedans.com

de combate, y los eventuales robots soldado, siempre permanezcan bajo el control de profesionales adecuadamente cualificados y acreditados.

Como siempre, la tecnología crea posibilidades y capacidades que, cuando se usan de forma malintencionada, descubren nuevas vulnerabilidades para una sociedad no educada ni concienciada para tales supuestos. En todo caso, la causa de los problemas hay que buscarla en la condición humana antes que en las nuevas tecnologías que, a la postre, solo son herramientas que, generalmente, llegan cargadas de beneficios para la colectividad.

Por un lado, los vehículos eléctricos y autónomos, provistos de los sensores adecuados a su misión operativa, ganarán presencia en las zonas de operaciones. Naturalmente, los datos generados por dichos sensores servirán para alimentar diversos algoritmos de *machine learning* propios de las diversas funciones del combate. Un papel muy relevante en esta operativa corresponderá a la hiperconectividad que proporcionarán las comunicaciones de nueva generación, como 5G, probablemente el mayor salto tecnológico de la historia de las telecomunicaciones.

Pero probablemente, los drones serán las plataformas autónomas con mayor impacto en la operativa diaria de los ejércitos. Los drones del mañana serán más furtivos, más rápidos, más computarizados, mejor equipados para la guerra electrónica, más letales, más autónomos y, en algunos casos, capaces de desplegar como grupos de minidrones. Los sensores ISR[32] serán mucho más inteligentes. La próxima generación desarrollará UAV[33] más rápidos, más maniobrables y tal vez sigilosos; incluso servirán de apoyo para los aviones de combate tripulados. Por supuesto, los algoritmos implementados permitirán a los drones llevar a cabo una gama mucho más amplia de funciones sin necesidad de intervención humana como la detección, selección de objetivos, puntería de armas, etc.

[32] ISR: *Intelligence, Surveillance and Recconaissance* (Inteligencia, Vigilancia y Reconocimiento).

[33] UAV: *Unmanned Aerial Vehicle* (Vehículo Aéreo no tripulado).

Figura 6. Plataforma Aérea Sensorizada de Inteligencia. Fuente. Ejército de Tierra.

En general, los desarrollos con Inteligencia Artificial permitirán que las plataformas autónomas no tripuladas puedan tomar más decisiones y realizar más funciones por sí mismas. El escenario más probable es que varios drones serán controlados por un solo humano, es decir, una persona realizará el mando y el control y los drones ejecutarán las funciones asignadas.

Los drones podrán abrirse camino en las áreas de mayor riesgo para reducir los riesgos de las aeronaves tripuladas, probar y desafiar las defensas antiaéreas, identificar y neutralizar francotiradores o aumentar considerablemente la capacidad ISR y de las armas de una misión dada.

En todo caso, con el horizonte de 2030 los algoritmos no permitirán que las plataformas no tripuladas puedan responder o reaccionar de forma autónoma a desarrollos imprevistos en un entorno dinámico y cambiante. Por otra parte, las doctrinas de los ejércitos exigirán por norma general que un humano se ocupe del mando y control ante un supuesto de uso de la fuerza letal.

El combatiente conectado

El incipiente mundo de los *wearables*[34] encuentra en la figura del combatiente un enorme entorno de experimentación y aplicación. Por una parte, la capacidad de capturar datos del entorno físico donde opera el soldado le convierten en un generador de datos con los que alimentar algoritmos de naturaleza táctica. Desde otro punto de vista, estos pequeños dispositivos permitirán monitorizar el estado de salud del combatiente y, por tanto, contar con datos objetivos para la detección y tratamiento de cualquier trastorno de sueño, salud cardiovascular e, incluso, salud mental.

Lógicamente, la existencia de un interés comercial en este tipo de soluciones conlleva que los sensores reduzcan progresivamente su tamaño y la precisión de sus datos en reducidos plazos de tiempo; al mismo tiempo, las baterías van aumentando su eficiencia.

Otra funcionalidad con la que ya se está experimentando son los *wearables* en forma de cámaras adosadas a la ropa que toman imágenes animadas a intervalos establecidos de manera automática de forma que, al final, se obtiene un video. *Google* ya ha lanzado un proyecto en esta línea mediante su producto *Google Clips*.

Todos estos avances redundarán en un combatiente mejor preparado y protegido, tanto en el transcurso de la preparación como durante la ejecución de sus misiones operativas. Pero, además, la disponibilidad de abundantes datos permitirá analizar las situaciones del combate y, en su caso, mejorar las técnicas y doctrinas en pro de mayores niveles de protección y eficacia del combatiente.

La sanidad

Indudablemente, el campo sanitario se presenta propicio a numerosos y revolucionarios cambios a los cuales no escapará la sanidad militar. El paradigma de la atención médica evolucionará hacia un futuro en el que no se recurrirá al sistema de salud únicamente al detectar síntomas de una enfermedad, sino que un conjunto de dispositivos y técnicas permitirán monitorizarla de manera continuada.

[34] *Wearable* es un dispositivo electrónico que el usuario puede llevar incorporado en su ropa.

En el trasfondo de esta revolución vuelven a aparecer los datos como combustible para entrenar algoritmos y conseguir que una máquina sea capaz de entender qué esconden esos datos en un tiempo próximo al real; por ejemplo, los datos capturados mediante radiografías, escáneres, tomografías, resonancias magnéticas, etc. El uso de herramientas de diagnóstico mediante imagen ha ido creciendo a lo largo del tiempo y, además de ser profusamente utilizado, supone un importante elemento de coste: donde antes un médico tenía que procesar manualmente unas pocas imágenes, ahora es perfectamente habitual que en una sola prueba se obtengan cientos de imágenes en finas capas, en procesos que pueden llegar a ser profundamente tediosos y que incrementan la probabilidad de error debido al cansancio o la pérdida de atención. Frente a ello, un algoritmo ofrece la capacidad de reconocer elementos de diagnóstico en una imagen; a medida que esos algoritmos son entrenados con más y más imágenes y sus posteriores resultados diagnósticos, esa posibilidad se convierte en una realidad. Es fácil imaginar los beneficios de estos diagnósticos para las fuerzas desplegadas en zonas de operaciones y asistidas desde cualquier lugar lejano.

Como se ha señalado anteriormente, los *wearables* tendrán un activo protagonismo en el nuevo modelo sanitario que podría describirse como «llevar al médico en la muñeca»: sensores no intrusivos de medición de glucosa, dispositivos para realizar analíticas con carácter preventivo o para confrontar con los datos genéticos del interesado, etc. En definitiva, un nuevo modelo de gestión de la salud basado en los datos de los miembros de la organización que son tratados por medio de algoritmos con la única finalidad de disponer de unos recursos humanos saludables y con todas sus capacidades.

El uso de pulseras de monitorización de la actividad física de los componentes de las fuerzas será otra realidad: cualquier ejército está interesado en disponer de recursos sanos y con hábitos de ejercicio más saludables.

El futuro apunta hacia un entorno cada vez más controlado en el que la mayoría de los riesgos puedan ser detectados de manera inmediata: un modelo de salud basado cada vez más en la prevención. Será el médico quien monitorice a sus pacientes y les contacte cuando sea necesario; su rol seguirá siendo imprescindible para evitar lecturas alarmistas de los datos proporcionados por los *wearables* o, en otros casos, para contextualizar la menor precisión de dichos dispositivos en comparación con los dispositivos de carácter profesional.

Las experiencias en esa dirección de una atención sanitaria preventiva son múltiples: cepillos de dientes conectados que deben utilizarse en combinación con una aplicación de teléfono inteligente para transmitir datos sobre los hábitos de higiene bucodental; pulseras u otro tipo de *wearables*, superficiales o insertados en el cuerpo, para detectar trastornos del sueño o eventos de hipertensión; pastillas que contienen sensores y que, al ser ingeridas, suministran variada información sobre el estado del individuo.

Claramente, la sensorización a cada vez más niveles supone una de las avenidas de investigación más interesantes en el mundo de la medicina. Esta ciencia se está redefiniendo en función de las posibilidades que proporciona la tecnología, y generando un entorno completamente diferente, que requerirá una drástica redefinición de muchos conceptos.

Tecnología, ética y herramientas para la Defensa: qué se ve más allá

Los años venideros serán testigo de una revolución tecnológica sin precedentes, caracterizada por la convergencia de una serie de tecnologías que se unen entre sí para generar productos y servicios inimaginables hace unos pocos años.

El Ministerio de Defensa, como el resto de las administraciones públicas, afronta un amplio abanico de desafíos que amenazan su viabilidad a largo plazo o la propia fortaleza de la institución en el marco de una sociedad digital[35]. Por tanto, debe pergeñar sus inversiones digitales con una visión estratégica de largo plazo a fin de prosperar en una

[35] *Entorno operativo 2035*. Disponible en:
http://www.ieee.es/Galerias/fichero/OtrasPublicaciones/Nacional/2019/entorno_operativo_2035.pdf
Panorama de tendencias geopolíticas. Horizonte 2040
http://www.ieee.es/Galerias/fichero/OtrasPublicaciones/Nacional/2019/panorama_de_tendencias_geopoliticas_2040.pdf

época de cambios exponenciales[36]. La planificación de dichas inversiones estratégicas debería comenzar hoy mismo. Naturalmente, dicha estrategia ha de difundirse convenientemente a las personas, como poseedoras del conocimiento sobre los procesos de la defensa y como encargadas de su ejecución; sin información y sin conocimiento de lo que se quiere alcanzar, sería difícil llegar al resultado propuesto[37].

La Alta Dirección debería asimilar e incorporar a su acervo y estilo de liderazgo que el futuro no es simplemente una cuestión de tecnología. Antes bien, es cuestión de curiosidad, de vocación por probarlo todo, de inquietud y de ganas de mejorar; el mañana es cuestión de actitud. Una organización que no sea capaz de crear y alimentar esa actitud en sus directivos se encontrará, antes o después, con problemas de viabilidad de difícil solución. Quien no lo perciba así, probablemente sea parte del problema antes que de la solución. Dado que las responsabilidades de dirección de las organizaciones cada vez tendrán menos de magia y más de ciencia, será necesario que dichos escalones sean capaces de valorar qué se puede pedir a un algoritmo, qué posibilidades reales tiene de generar resultados tangibles o qué tiempos de desarrollo cabe esperar en un proyecto basado en datos.

La transformación digital ha comenzado en las empresas de todo el mundo y las organizaciones deben convertirse en *Data-Driven Decisions Companies*. Esta es una nueva era donde el big data no solo ha suministrado a las tecnologías de *machine learning*, sino que está llegando el tiempo de la Inteligencia Artificial, con plataformas que utilizan redes neuronales con *deep learning*[38] para evolucionar hacia las *AI*[39] *Driven-Decisions Companies*. La Inteligencia Artificial supone una auténtica revolución tecnológica con implicaciones éticas y sociales para cualquier actividad humana. Requiere de profundas reflexiones sobre hacia dónde se dirige el mundo, los principios éticos asociados al desarrollo de sus algoritmos y, en definitiva, las reglas que deben presidir la evolución de estas tecnologías. Dichas reflexiones deben desarrollarse en todos los ámbitos, de forma realista y alejada del tremendismo. Como en tantas otras

[36] Gartner Inc. How the Operating Model for Government in 2030 Drives Actions Today. 2018.

[37] MARTÍN DE LOPE, Luis Ignacio. Conocimiento: Factor crítico para ejecutar la estrategia. itSMF España. 2012.

[38] *Deep learning* consiste en un aprendizaje profundo es una clase de algoritmos ideados para el *machine learning*.

[39] AI: *Artificial Intelligence* (Inteligencia Artificial)

ocasiones, muchos de los problemas que surgen alrededor de la tecnología no tienen su origen en que sea diseñada con objetivos potencialmente perjudiciales, sino en el hecho de que sea gestionada de manera incorrecta, con un nivel deficiente de seguridad, con graves errores en los procedimientos o ignorando que en el mundo existen personas malintencionadas o con oscuros intereses. Para dicho análisis parece imprescindible contar con personas que tengan profundos conocimientos en la materia y ponerse a salvo de los miedos irracionales, la desinformación, la demagogia o el populismo. Buena parte del futuro de la sociedad está en juego con el establecimiento de principios razonables y con sentido a la hora del desarrollo de algoritmos de Inteligencia Artificial.

Otras tecnologías concurrirán con la Inteligencia Artificial para reconfigurar de manera irreversible los procesos, productos y servicios del ámbito de la Defensa. Contar con los mejores profesionales es importante, pero la clave está en el hecho de reconfigurar las actividades y procesos de dicho ámbito, de modo que permitan generar datos estructurados que puedan ser utilizados para entrenar a los correspondientes algoritmos. Naturalmente, el aseguramiento de todo el caudal de datos a tratar por los nuevos algoritmos constituye un desafío mayúsculo.

Por supuesto, las implicaciones de esta ola de innovación son muchas y profundas. Entre otras cosas, la sociedad del futuro tendrá que repensar y replantear el concepto de trabajo; tendrá que delimitar cuál es el espacio de las personas y cuál el de las máquinas. ¿Y si el desarrollo de la Inteligencia Artificial, en realidad, terminara creando muchos más puestos de trabajo de los que elimina, como postulan algunos estudios llevados a cabo por Gartner o permitiese que los trabajos existentes añadiesen más valor?, ¿y si la automatización de los trabajos resultara ser la clave para el progreso de la sociedad?

Aunque la eliminación de determinados trabajos es susceptible de generar tensiones sociales, en el caso específico de los procesos de negocio de la Defensa, la abundancia de tareas peligrosas justifica sobradamente la introducción de este conjunto de tecnologías. Esta transformación generará una defensa más eficaz y más eficiente, se podrán ajustar los efectivos humanos para focalizarlos en tareas de mayor valor y se mejorará la protección de las fuerzas.

Una nueva defensa para una incipiente sociedad digital en la que, como afirmó el escritor Alvin Toffler[40]: «Los analfabetos del siglo XXI no serán aquellos que no sepan leer o escribir, sino aquellos que no puedan aprender, desaprender y reaprender».

*Jesús Gómez Ruedas**
Coronel (R)

[40] Alvin Toffler, escritor y futurista estadounidense.