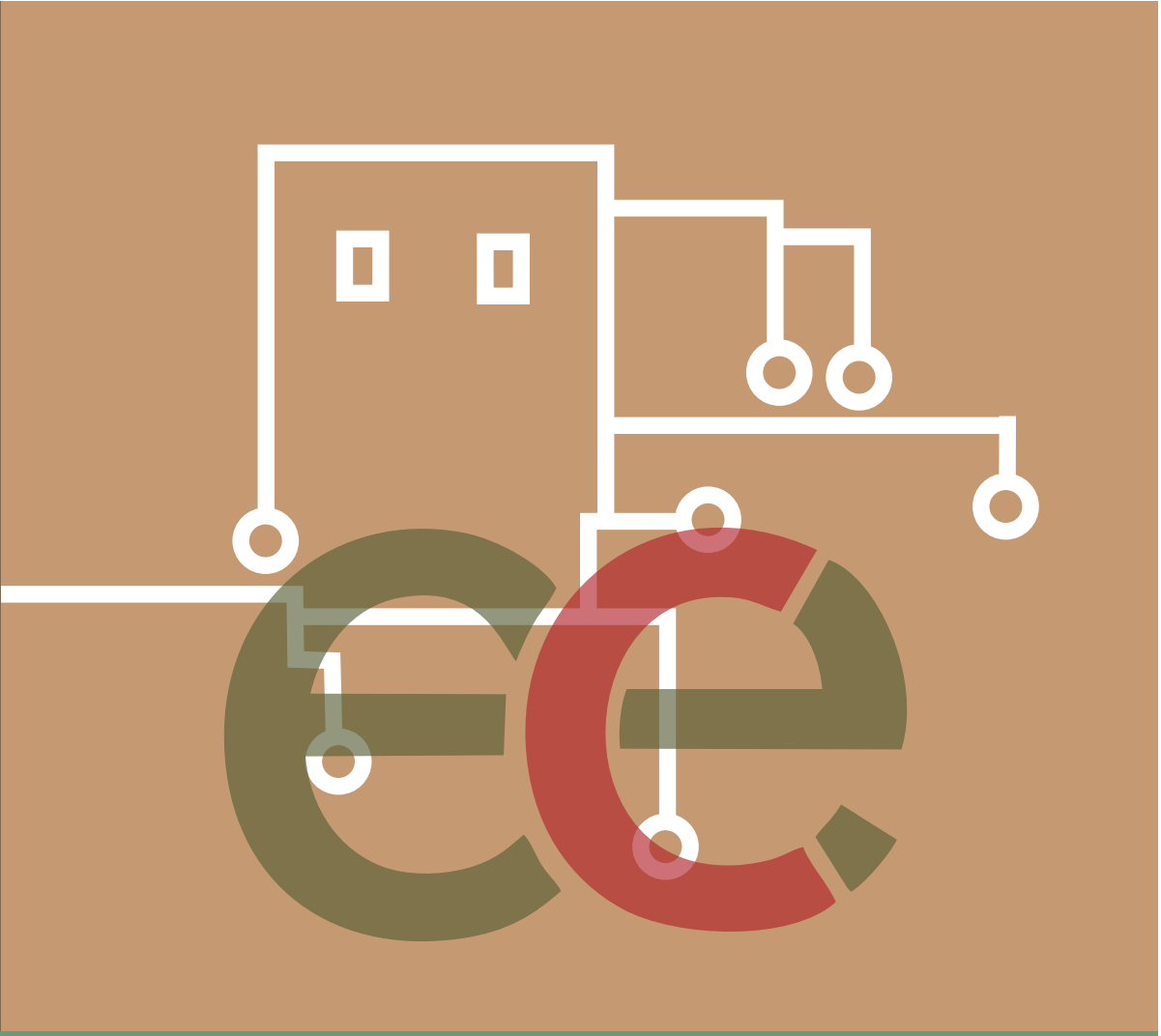


Miguel Blanco Souto (coord.)

Una alianza estratégica para el entorno 2035

I Congreso Ejército, Empresa y Conocimiento

UNIVERSIDAD DE GRANADA
MANDO DE ADIESTRAMIENTO Y DOCTRINA

UNA ALIANZA ESTRATÉGICA PARA EL ENTORNO 2035

I CONGRESO EJÉRCITO, EMPRESA Y CONOCIMIENTO

Miguel Blanco Souto
(Coord.)

UNA ALIANZA ESTRATÉGICA PARA EL ENTORNO 2035

I CONGRESO EJÉRCITO, EMPRESA Y CONOCIMIENTO

Transcripción y traducción: Ana María Corchero Fernández

GRANADA
2020

Colección Emilio Herrera

El Centro Mixto UGR-MADOC no se responsabiliza de las opiniones de los autores.

ISBN: 978-84-338-6741-4
Edita: Editorial Universidad de Granada
Campus Universitario de Cartuja. Granada
Colegio Máximo, s.n., 18071. Granada
Telf.: 958 243930-246220
Web: editorial.ugr.es
Fotocomposición: María José García Sanchis. Granada
Diseño de cubierta: Josemaría Medina Alvea. Granada

Indice

Panel 5

LAS NUEVAS INICIATIVAS EN EL ÁMBITO DE LA INVESTIGACIÓN Y DESARROLLO. POSIBILIDADES DE FINANCIACIÓN

Prólogo

El 22 de marzo de 2017 la ciudad de Granada recibió el nombramiento de «Ciudad de la Ciencia y la Innovación», otorgado por el Ministerio de Economía, Industria y Competitividad. Desde entonces, las principales instituciones de la ciudad han venido patrocinando actividades que suponen un impulso a la investigación en los ámbitos empresarial y universitario. La Universidad de Granada y el Mando de Adiestramiento y Doctrina no podían permanecer ajenos a esta realidad y, fruto de su compromiso con la innovación y con la ciudad, nació el «*I Congreso Ejército, Empresa y Conocimiento. Una alianza estratégica para el horizonte 2035*».

En el ámbito científico, el sector de la defensa ofrece unas enormes posibilidades que se ven potenciadas por las circunstancias que vive el mundo en general y Europa en particular. Circunstancias que están conduciendo a la Unión Europea a prestar una mayor atención a su propia defensa y, consecuentemente, a invertir si no más, sí al menos de una manera más eficiente en este campo. Esta mayor atención se traduce en posibilidades muy interesantes en el ámbito de la investigación científica y en la transferencia de conocimiento. Posibilidades que Granada, de la mano de la Universidad y del MADOC, no puede dejar pasar y en las que puede jugar un papel muy relevante, motivo por el cual ambas instituciones se implicaron en la organización del Congreso como punto de partida para colaboraciones futuras dentro de este ámbito.

Un aspecto muy destacable de este evento fue la participación e implicación de las empresas del sector de la defensa. El esfuerzo de Ejército y Universidad no resultaría productivo si no hubiera un sector empresarial capaz de impulsar la investigación y materializar sus resultados. El papel de la industria de defensa en el proceso de modernización del Ejército de Tierra es fundamental

para dotar a la Fuerza 2035 de la tecnología necesaria para alcanzar las capacidades requeridas, de modo que pueda hacer frente con éxito a los retos de un entorno operativo muy complejo.

La calidad e interés de las distintas ponencias aconsejaban su publicación, facilitando así el acceso a ellas de quienes pudieran tener interés en estos asuntos.

Con este libro, el Centro Mixto UGR-MADOC inaugura la Colección Editorial Emilio Herrera, que recupera el nombre de quien fuera insigne militar y brillante científico, representando a la perfección los valores que subyacen tras la colaboración entre Universidad y Ejército. El nacimiento de esta colección, que pretende dar cabida a trabajos relacionados con el ámbito tecnológico de interés para la defensa, supone un paso más en la colaboración de dos instituciones que han sabido hacer de sus diferentes ámbitos de actuación, conocimientos y experiencias una fuente de enriquecimiento.

Jerónimo de Gregorio y Monmeneu
Teniente General Jefe del MADOC

Prólogo

La Universidad de Granada, en su firme compromiso con la sociedad, y aprovechando la ya dilatada colaboración con el Mando de Adiestramiento y Doctrina del Ejército, quiso impulsar junto al MADOC el «*I Congreso Ejército, Empresa y Conocimiento. Una alianza estratégica para el horizonte 2035*», celebrado en octubre de 2020. El Congreso abordó las necesidades de investigación del Ejército de Tierra para el año 2035, así como las capacidades que podía ofrecer la Universidad de Granada.

El sector de la defensa, muy presente en el mundo universitario internacional, ha ido adquiriendo un mayor protagonismo en el ámbito científico y universitario español. A ello se une, que la Universidad de Granada se ha convertido en un referente clave en temas de seguridad y defensa gracias a la colaboración con el MADOC desde hace más de dos décadas y media. Desde entonces, las redes académicas y profesionales construidas a nivel nacional e internacional han supuesto un importante valor añadido para la investigación en estos campos.

Para dar una continuidad a esta destacada trayectoria, la Universidad y el MADOC, no dudaron en sumarse al impulso de las instituciones granadinas en promover la investigación y seguir generando espacios sinérgicos, desde que en el año 2017 se distinguiera a Granada como «Ciudad de la Ciencia y la Innovación» por el Ministerio de Economía, Industria y Competitividad.

En consecuencia, el Congreso se articuló de modo que la investigación en cuestiones de seguridad y defensa constituyeran uno de los ejes principales para concederle el impulso perseguido. Las temáticas fueron amplias y los expertos de referencia del mundo universitario, militar, empresarial y político con los que se contó, profundizaron, debatieron e intercambiaron ideas que propiciarán la transferencia de conocimiento.

El éxito del Congreso y la calidad de las intervenciones aconsejaron que éstas fueran publicadas para darles la adecuada divulgación. En este sentido, el presente libro constituye un hito en las publicaciones del CEMIX, toda vez que con él comienza una nueva colección de contenido científico-tecnológico en el ámbito de la seguridad y la defensa: la Colección Editorial Emilio Herrera. Militar granadino y científico de gran prestigio internacional, fue reconocido por la Universidad de Granada en el año 2017 inaugurando una estatua en su memoria. Emilio Herrera representa esa simbiosis entre militar y científico, el perfecto militar ilustrado a imagen de Francisco Javier de Balmis quien vivió en el siglo XVIII-XIX, también traído recientemente a la memoria con la «operación Balmis» después del escenario que nos ha tocado vivir con la pandemia global del COVID. Esta circunstancia nos recuerda la importancia de la investigación científica y de la colaboración entre todas las instituciones. Ellos representan esa cooperación y asistencia entre mundo civil y mundo militar que quiso dar a conocer el Congreso, así como la alianza estratégica en un panorama de incertidumbre como es el año 2020.

Pilar Aranda Ramírez
Rectora Magnífica de la Universidad de Granada

Introducción

El *I Congreso Ejército, Empresa y Conocimiento. Una alianza estratégica para el horizonte 2035*, organizado conjuntamente por el Mando de Adiestramiento y Doctrina del Ejército de Tierra (MADOC) y la Universidad de Granada, se planificó para lograr la consecución de unos ambiciosos objetivos estratégicos de interés para ambas instituciones. Por una parte, se pretendió mostrar a la ciudad de Granada que la defensa es un pilar fundamental para el desarrollo empresarial, con la intención de facilitar la implantación en la provincia de empresas pertenecientes a este sector emergente, clave en inversiones y tecnología y potencial dinamizador del mercado laboral. Por otra, se trató de fomentar la investigación en asuntos militares para proporcionar al Ejército de Tierra las mejores soluciones a los retos que plantea el nuevo entorno operativo futuro y para que esta institución se pueda aprovechar de los avances en tecnología de doble uso. Y por último, constituyó un objetivo de especial interés el fomento de la investigación conjunta entre la Universidad, las empresas del sector de la defensa y el MADOC en las áreas de organización, liderazgo y dotación de nuevos materiales dentro del ámbito del Ejército de Tierra.

Para tratar de alcanzar la consecución de estos objetivos estratégicos, el Congreso se organizó en cinco paneles en los que destacados expertos abordaron las necesidades de investigación del Ejército, las capacidades de la Universidad de Granada, las capacidades de las empresas del sector de la defensa y las posibilidades de financiación.

En primer lugar se presentaron los retos de seguridad y defensa global a los que debemos enfrentarnos en el entorno operativo futuro de 2035, los retos que debe afrontar el Ejército de Tierra para operar en los nuevos escenarios y los retos tecnológicos en el ámbito de la Universidad y en el ámbito empresarial.

En un segundo panel se trataron las posibilidades que ofrecen las nuevas tecnologías, tales como la inteligencia artificial y el *big data,* para atender a las necesidades del Ejército de Tierra, teniendo en cuenta las magníficas capacidades tecnológicas de las que dispone la empresa del ámbito de la defensa y la Universidad de Granada, analizadas también desde un enfoque humanista.

En un tercer panel se presentaron las soluciones tecnológicas que algunos ejércitos aliados están adoptando para adaptarse a los nuevos escenarios, derivadas de sus particulares procesos de investigación, con el objetivo de mejorar su eficiencia.

En un cuarto panel, centrado en la tecnología y nuevos materiales tales como robótica, drones, nanotecnología y realidad aumentada, se expusieron las necesidades del Ejército de Tierra, las capacidades de las empresas españolas, las capacidades de la Universidad de Granada y de otras universidades y algunos de los proyectos de investigación actualmente en curso.

En el quinto y último panel se plantearon las nuevas iniciativas en el ámbito de investigación y desarrollo en proyectos de defensa y las posibilidades de financiación nacionales y europeas, así como iniciativas en el ámbito de investigación empresarial y en el de desarrollo industrial a nivel nacional y autonómico.

Los objetivos de este Congreso fueron ciertamente ambiciosos, pero el interés y la relevancia de los temas tratados justificaron sin duda ese elevado nivel de ambición.

PANEL I

RETOS FUTUROS

Seguridad y defensa global

Rafael Estrella Pedrola
Vicepresidente del Real Instituto Elcano

La seguridad y la defensa global se sitúan hoy en un marco multiconceptual. Hablar hoy de crisis no tiene el mismo sentido que hace un cuarto de siglo. Blake Snyder[1] define el concepto de crisis como «una secuencia de interacciones entre los gobiernos que conllevan una peligrosamente alta probabilidad de guerra». Hoy en día esta definición de crisis es incompleta. Vale para la seguridad de un estado frente a sus vecinos, pero la noción de crisis tiene un sentido más amplio y mucho más complejo, al igual que la noción de seguridad y de guerra. Hoy las guerras no se declaran; los conflictos son intraestados y crecientemente con actores no estatales; se producen por razones étnicas, religiosas, por el acceso a los recursos, etc.; son asimétricos entre un estado y una organización no estatal o un grupo terrorista o insurgente, donde ganar no significa necesariamente derrotar; son crecientemente híbridos, donde los actores utilizan una panoplia de instrumentos que van desde el combate al terrorismo, narcotráfico, el uso de internet, etc. En los conflictos armados clásicos la mayoría de las víctimas son los propios combatientes, aunque también se produzcan víctimas civiles. En cambio, los nuevos tipos de conflicto provocan un alto porcentaje de víctimas civiles así como una gran cantidad de refugiados y desplazados, tal y como se puede observar en los que están teniendo lugar actualmente en Sudan del Sur, Siria o África.

También las amenazas a la seguridad actual son de otra naturaleza. Recientemente el Instituto El Cano ha realizado una encuesta en España con la intención de conocer cuáles son las

1. Guionista, consultor, autor y educador estadounidense.

amenazas globales que perciben los españoles, y por vez primera el cambio climático aparece de manera destacada como la principal amenaza percibida, a la que se vinculan (o no) pandemias, hambrunas, sequías, inundaciones y otros males. Además de esta se perciben otras amenazas, tales como terrorismo, tráficos ilícitos y retos vinculados a la ciberseguridad y a los avances tecnológicos.

Una característica de este tiempo es que el conocimiento se extiende de una manera rapidísima por todo el mundo. Personalmente, estoy convencido de que la tecnología 5G llegará a África en un plazo no superior a quince años y que se extenderá en un porcentaje muy próximo al que tenemos en Europa.

Hay otras amenazas derivadas de las asimetrías económicas dentro de los países o entre países, las cuales son mucho más visibles en un mundo globalizado y que tienen como corolario las migraciones. Existen amenazas al orden global, como la quiebra del sistema de comercio de la Organización Mundial del Comercio (OMC) o la ruptura de los regímenes de control de armamento. Todo ello en un entorno complejo que reduce la capacidad de actuación concertada en algunas materias.

Vivimos, por lo tanto, en lo que Habermas[2] ha denominado como «una comunidad involuntaria de riesgo constante». Se creía que con el fin de la Guerra Fría la globalización y la interdependencia sin restricciones ideológicas actuarían como factores de seguridad que protegerían los intereses mutuos e impulsarían el multilateralismo. El multilateralismo permitió prevenir la proliferación nuclear y favoreció el crecimiento y la prosperidad hasta llegar a niveles sin precedentes en muchos países del mundo, como, por ejemplo, China, que cuando se incorporó en 2001 a la OMC eliminó de golpe siete mil limitaciones de tipo arancelario a la importación de productos. Hoy China no sería la superpotencia que es sin esa acción de apertura comercial. Pero también el multilateralismo ha permitido y permite juzgar a genocidas o responsables de crímenes contra la humanidad. Ese impulso nos permitía ser más eficaces contra nuevas amenazas que no conocen fronteras (cambio climático, migraciones, etc.). Ese impulso multilateral es, por ejemplo, el que permitió celebrar un acuerdo en-

2. Filósofo y sociólogo alemán reconocido en todo el mundo por sus trabajos en filosofía política y del lenguaje, ética y teoría del derecho.

tre China y los Estados Unidos sobre ciberseguridad con carácter previo a la celebración de la Cumbre de París en 2015 relacionada con el cambio climático y que facilitó la firma de un acuerdo.

Pero la realidad es que, hoy en día, el multilateralismo está en crisis; o mejor dicho, está siendo seriamente cuestionado. El orden mundial que conocíamos desde finales de siglo pasado ya no existe y no ha sido sustituido por otro orden sino por un esquema de competencia entre grandes potencias para el que los estadounidenses no estaban preparados y los europeos, desde luego, tampoco. Una competencia que no significa necesariamente hostilidad. En este escenario habría que destacar que los Estados Unidos siguen siendo un actor que goza de una ventaja asimétrica con respecto a Rusia y China, y no es otra que contar con potentes aliados. Algo que los Estados Unidos parecen estar dejando de lado. Los indicios de esta nueva situación son los cambios geopolíticos, la rivalidad entre potencias que quiebran la cooperación a nivel global, las tensiones internas y el cuestionamiento de una sociedad avanzada, entre otros.

Tras el fin de la Guerra Fría pasamos de un mundo bipolar a un mundo unipolar y ahora se está dando paso a un mundo multipolar asimétrico. No estamos en «el fin de la historia» que había anunciado Fukuyama[3] ni tampoco en contra de lo que dijo Huntington[4] sobre la condición de los Estados Unidos como «superpotencia solitaria».

Los elementos más destacados que amenazan el multilateralismo, con un importante efecto sobre Europa, son las tensiones entre los Estados Unidos y China (no solo en el ámbito económico), los conflictos en el mar de China y la anexión de Crimea por parte de Rusia en 2014, que supuso un antes y un después toda vez que fue una ruptura del marco de acuerdos multilaterales y dinamitó la colaboración regional en materia de seguridad en que la OTAN y Rusia trabajaban con la perspectiva de ser socios en la seguridad y la estabilidad de Europa. Las tensiones entre los Estados Unidos y Rusia han hecho y están haciendo un daño grave al sistema de control de armamento y al régimen de no proliferación.

3. Politólogo estadounidense que ha escrito una variedad de temas en el área de desarrollo y política internacional.

4. Politólogo y profesor de ciencias políticas en el Eaton College y Director del Instituto John M. Olin de Estudios Estratégicos de la Universidad de Harvard.

Además asistimos en todo el mundo a un creciente nacionalismo populista, en Europa de una forma muy visible al igual que en los Estados Unidos, donde está gobernando y donde se está cuestionando el multiculturalismo, la cooperación global y elementos fundamentales tales como las fronteras abiertas. Con Donald Trump los Estados Unidos han abandonado o parece que quieren abandonar su rol tradicional como principales defensores del orden liberal y aparecen como enemigos de la cooperación global, a la que han situado como antítesis del patriotismo (patriotismo vs. globalismo). Pese a ello hay que decir que la cooperación sigue siendo importante y eficaz en diversos ámbitos, como por ejemplo en la lucha contra el cambio climático. La retirada de los Estados Unidos no ha tenido apenas seguidores, se sigue avanzando y se están dando pasos importantes. En los propios Estados Unidos y en el resto de mundo las redes de ciudades comprometidas con el cambio climático son especialmente activas e importantes y están dando resultados.

En los últimos tiempos se han producido avances importantes en cooperación internacional, como por ejemplo la convención sobre armas químicas, que fue negociada en la Guerra Fría y que entró en vigor a partir de 1997, de la que forman parte ciento noventa estados que suponen el 98% de la población mundial. Esta convención, a pesar de no tener capacidad de sanción, articuló un mecanismo (*Name&Shame*[5]) que ha permitido verificar la destrucción de un 97% de este tipo de armas, aunque naturalmente no ha acabado con ellas, tal y como hemos visto en acciones de grupos terroristas en Siria o en Tokio

El desarrollo tecnológico es tal vez el más claro ejemplo de un ámbito que ofrece enormes oportunidades y a la vez plantea serias amenazas. Cisco Systems estima que en 2022 habrá veintiocho mil millones de dispositivos electrónicos conectados a internet en un mundo de siete mil quinientos millones de habitantes. En 2030 serán ya quinientos mil millones de aparatos conectados. Nunca ha sido tan fácil colaborar, innovar y compartir información, la moneda más valiosa en la era digital, pero nunca ha sido más fácil la acción disruptiva, manipular y explotar vulnerabilidades con efectos devastadores. El coste de estos ataques no es solo econó-

5. Nombrar y avergonzar. Consiste en hacer pública la actuación incorrecta de una persona, grupo o empresa.

mico sino que también afecta a la privacidad, a la seguridad de los estados, a infraestructuras críticas e incluso a las capacidades de defensa y a los procesos electorales. Desde los ciberataques producidos en Estonia en 2007 y en Georgia en 2008 la OTAN viene protegiendo sus infraestructuras. En la Cumbre de Gales de 2014 la OTAN acordó una política de ciberdefensa y puso en marcha un plan de acción en cuya estrategia de planeamiento se considera que un ciberataque podría constituir un ataque armado en determinadas circunstancias, y en consecuencia podría acarrear la invocación del artículo quinto del Tratado de Washington de defensa colectiva. Pero quizás una de las características más importantes de este plan de acción es que la OTAN ha puesto en marcha el NATO Industry Cyber Partnership (NICP), lo que supone una sólida cooperación con el sector privado para luchar contra las amenazas y desafíos en este ámbito.

Otro ejemplo importante de la relevancia y de la eficacia del multilateralismo es la coalición mundial contra el Daesh, compuesta por un ejército de estados voluntarios (empezaron siendo una veintena y hoy son ochenta) que se puso en marcha en el 2014 con cinco grupos de trabajo: uno de operaciones militares, otro dedicado a cómo contrarrestar la propaganda del Daesh, otro a quebrar las infraestructuras financieras, otro a prevenir los desplazamientos de los terroristas del Daesh a través de las fronteras y un quinto grupo para apoyar la restauración de las áreas liberadas. Uno de los efectos más visibles de esta intervención es que la difusión de propaganda de la organización terrorista cayó entre el 2015 y el 2017 en un 85%.

Pero sin duda para la OTAN y para los europeos el mayor test de estrés ha sido la acción de Rusia en Ucrania y la anexión de Crimea. Rusia está dispuesta y es capaz de poner en cuestión un orden europeo basado en reglas comúnmente aceptadas en el que ya no toma parte. Desde entonces Rusia viene practicando una acción desestabilizadora con continuos actos de provocación, ejercicios no anunciados en las fronteras, ataques híbridos, cuestionamiento de control de armas, interferencias en procesos electorales o acciones en el mundo digital. Todo ello convierte a Rusia en la principal amenaza híbrida para Europa, con un área de influencia de límites difusos.

En cuanto a China, está demostrando su potencial como amenaza híbrida en su propia área de influencia en Asia. Apuesta por

el multilateralismo y eso lo diferencia de Rusia, pero siempre y cuando le permita asegurar su crecimiento económico, aumentar su influencia geopolítica y proteger sus intereses de seguridad.

La Estrategia de Seguridad de los Estados Unidos dice que China y Rusia quieren construir un mundo acorde con su modelo autoritario. Conceptualmente ninguno de estos dos países tiene una ideología exportable. Rusia tiene una vocación disruptiva y apoya a populismos de derechas y de izquierdas, mientras que China se relaciona con los gobiernos y no interfiere en la política de otros países. También son diferentes por su dimensión, por su potencial, por su población, por su economía (China es ya el primer exportador mundial), por gasto militar (muy superior en el caso de China) y por su comportamiento global. Incluso es posible que Rusia siga teniendo y modernizando un arsenal nuclear con el fin de hacer creíble su capacidad de amenaza o de disuasión, cosa por la que China no opta o no ha optado por propia elección. Rusia nunca será más potente que China ni que la Unión Europea, pero es cierto que es la amenaza más cercana. El rol destacado que Rusia está teniendo en Asia Central, concretamente en Siria, está aumentando su prestigio y su reputación y está causando una acción disruptiva en Europa. La respuesta ante esto no puede ser otra que adoptar un conjunto de medidas de defensa, de disuasión y de seguridad y potenciar una solidaridad férrea entre los componentes de la Alianza Atlántica que garantice la defensa de todos y cada uno de ellos y su presencia avanzada. Se dice que la Unión Europea es altamente dependiente del gas y del petróleo ruso, lo cual es cierto, pero también es cierto que Rusia no es menos vulnerable: el gas y el petróleo suponen el 47% de sus exportaciones totales y el 40% de los ingresos del estado. Es decir, un cierre del grifo tendría efectos devastadores también para Rusia. China es y será una gran potencia, con acciones cuestionables y/o discutibles. Personalmente, la Belt&Road Initiative [6] no la concibo como una iniciativa multilateral sino como una acción de presencia y proyección económica por parte de China, que se siente incómoda en un marco de influencia que considera ya estrecho.

6. Iniciativa *Belt&Road*, referida a la franja económica de la Ruta de la Seda y la Ruta Marítima del siglo XXI.

Y finalmente me gustaría comentar dos cosas sobre la Unión Europea. En el tema del desarrollo de avances tecnológicos la Unión Europea se encuentra en tierra de nadie. Entre los avances de los Estados Unidos y China, la Unión Europea se encuentra retrasada y sin agenda de innovación, ya que todavía no ha sido capaz de conseguir un sistema digital único. En el mundo hay «compañías de fronteras» (por usar la expresión de la Organización para la Cooperación y Desarrollo Económico, OCDE) que representan la mayor parte de la productividad y que crean la mayoría de los puestos cualificados y mejor pagados. Europa tendría que seguir esa senda: las instituciones académicas, la industria, el sector financiero, los emprendedores, etc. En el futuro, el modo de medir el rendimiento de una institución académica será, posiblemente, mediante el número de *startups* lanzadas, los puestos de trabajo creados, la contribución al PIB local o regional, etc.

En cuanto a Europa y su seguridad, la Unión Europea se plantea si los Estados Unidos están retirándose del mundo. En una tormentosa cumbre de la OTAN en 2018, tras reclamar un gasto en defensa del 2% por parte de todos los socios, Donald Trump pronunció aquello de que «los Estados Unidos irían por su cuenta». Acaban de retirarse de Siria (espacio que ha sido ocupado por Rusia), han dinamitado el acuerdo con Irán, han abandonado o están abandonando a aliados que no estuvieron en Normandía pero sí que estuvieron con ellos en Siria, han anunciado su retirada de Afganistán, han anunciado la posibilidad de retirar las tropas en Corea del Sur, etc. Los Estados Unidos ya no son percibidos como una garantía de seguridad y algo va mal cuando critican a aliados como Canadá, Alemania o la Unión Europea y alaban a dirigentes liberales de Brasil y Filipinas, por no mencionar a Arabia Saudí. Esa demonización de lo que Trump llama «ideología del globalismo» supone que se aleja de la corriente de sus propios aliados. Todo esto tiene impacto en las relaciones trasatlánticas y en la percepción de los europeos de que deben defenderse solos en una era de competencia entre grandes potencias sin estar preparados para ello. Y ese va a ser el reto de la nueva Comisión: avanzar en la autonomía estratégica europea, que no es emancipación sino asunción de más responsabilidades. Y a la vista de que Trump dice que «los Estados Unidos no pueden ejercer de policía mundial», plantearse si debe haber una separación o una actualización de la relación.

En la actualidad hay un debate sobre la conformación de un ejército europeo. Las tres cuartas partes de los europeos están a favor de una política común de seguridad y defensa pero no de un ejército europeo, sino en todo caso, como dijo la actual presidenta de la Comisión Europea, de un «ejército de los europeos». Trump es distorsivo, los Estados Unidos son los líderes del mercado de seguridad, son hacedores de reglas y tratan de fijar las reglas de enfrentamiento, mientras que la Unión Europea avanza con el Fondo Europeo de Defensa (EDF)[7], con la Cooperación Permanente Estructurada (PESCO)[8], con la revisión anual de la coordinación de defensa, etc. Pero la realidad es que la Unión Europea no tiene capacidad de jugar un papel significativo en los asuntos globales. Debemos intentar seguir siendo transatlánticos, pero sobre todo más europeos.

7. *European Defence Fund.*
8. *Permanent Structured Cooperation.*

Análisis del Entorno Operativo Terrestre Futuro 2035

Antonio Ruiz Benítez

General de División
Director de Investigación, Doctrina, Orgánica y Materiales del Mando de Adiestramiento y Doctrina del Ejército de Tierra

Todos somos conscientes de los cambios relevantes que en poco tiempo ha experimentado nuestro entorno. Hoy el mundo global está hiperconectado y ello permite que sucesos ocurridos en los lugares más remotos tengan efecto en cualquier parte del planeta. Las redes sociales son capaces de difundir de forma instantánea, y no siempre con fundamento, comunicaciones, noticias e interpretaciones que crean opinión.

Estos cambios, que si bien nos facilitan la vida, transmiten conocimientos, permiten un contacto inmediato, aportan entretenimiento, favorecen gestiones, ahorran tiempo, crean empleos, ponen al alcance de la mayoría avances científicos y contenidos culturales que antes eran privilegios de muy pocos; conllevan también riesgos asociados. Multitud de agentes pueden aprovechar unos avances que permiten, por ejemplo, que grandes corporaciones dispongan de datos personales para darles un empleo que escapa al control de sus legítimos titulares. Tampoco podemos obviar las campañas de difusión que, empleando las redes sociales, pretenden influir y confundir a la opinión pública, creando desconfianza en las instituciones o mayor debilidad en países que ya de por sí son suficientemente inestables.

Los Ejércitos no pueden ser ajenos a este proceso y así, su preparación debe evolucionar al ritmo de los acontecimientos en el ámbito de la seguridad y adelantarse a ellos siempre que sea posible, mediante un continuo esfuerzo de investigación prospectiva, para poder responder con eficacia a los nuevos retos que se les planteen. Al igual que los Ejércitos de nuestro entorno, el Ejército de Tierra español asumió la tarea de definir el entorno operativo terrestre en un horizonte a medio plazo (año 2035), enmarcado dentro de los trabajos previos para contribuir al diseño de la

Brigada Experimental (BRIEX) en ese horizonte temporal. Este es uno de los procesos de transformación más importantes de su historia contemporánea. La Dirección de Investigación, Doctrina, Orgánica y Materiales (DIDOM) del Mando de Adiestramiento y Doctrina (MADOC) fue la unidad a la que se asignó la tarea de realizar un trabajo prospectivo para tratar de visualizar cómo podría ser el escenario en 2035 y plasmarlo en un documento denominado Entorno Operativo Terrestre Futuro para el año 2035. Así que nos pusimos en marcha para elaborar un producto final que nos brindara un documento de reflexión que actualizase los escenarios operativos futuribles y la actuación potencial del Ejército de Tierra en un horizonte de quince años (horizonte que coincide con el ciclo de planeamiento de Defensa a medio plazo), para posteriormente describir también las posibles visiones, cometidos y cambios. Estos son los aspectos más importantes de ese trabajo, en el que ha participado un numeroso grupo de expertos civiles y militares, entre los que cabe resaltar los pertenecientes al Grupo de Estudios de Seguridad Internacional (GESI) de la Universidad de Granada.

En el futuro, los escenarios de riesgo ya no se corresponderán exclusivamente con los tradicionales escenarios bélicos convencionales que oponían a ejércitos contendientes en un campo de batalla, y el enfrentamiento ya no será privativo exclusivamente de los ejércitos, sino que afectará de manera directa a toda la sociedad en su conjunto. Si apenas veinte años atrás se le hubiese consultado por el futuro a algún analista prospectivo, a buen seguro que no habría sido capaz de prever alguno de los acontecimientos más recientes. El ataque del 11S a los Estados Unidos (producido en su territorio por vez primera desde el ataque a Pearl Harbor), la primavera árabe, la anexión de Crimea por parte de Rusia, el acceso a la presidencia de los Estados Unidos del señor Trump o el Brexit, por poner algún ejemplo, dan una idea clara de que el futuro es impredecible y que, tal y como decía un filósofo, «solo está en manos de los dioses». También decía Darwin que «las especies que sobreviven no son las más fuertes, ni las más rápidas, ni las más inteligentes, sino aquellas que se adaptan mejor al cambio», por lo que la facultad de adaptación es clave para el éxito; y para conseguirlo no podemos limitarnos a actuar de forma reactiva.

El mundo actual es un mundo global caracterizado por la velocidad del cambio, en el que cada vez es más frecuente la apari-

ción de hechos disruptivos (especialmente de la mano de las nuevas tecnologías) o de actores no estatales, capaces de convertirse en riesgos y amenazas poliédricas cambiantes y difíciles de evaluar y predecir. Los recientes documentos de análisis prospectivo sobre el futuro escenario geopolítico y de seguridad mundial describen el entorno operativo futuro en base a cuatro características principales: volatilidad, incertidumbre, complejidad y ambigüedad. La velocidad con la que se producirán los cambios y la multiplicidad de actores que van a participar en un mundo global e interconectado, van a difuminar la distinción entre situaciones de paz y de guerra e incluso la atribución de acciones y la identificación de adversarios y de sus verdaderas intenciones. En este entorno global influirán dos grandes bloques de circunstancias: la dinámica entre las grandes potencias y las relaciones intrasocietales.

En cuanto al primer bloque, es muy probable que en el horizonte 2035 la rivalidad entre las grandes potencias siga siendo una constante y que el protagonismo se traslade hacia la región de Asia-Pacífico. A pesar de que parece probable que los Estados Unidos sigan manteniendo una supremacía militar, surgirán una serie de potencias que competirán con ellos política y económicamente.

En relación con las dinámicas intrasocietales, no podemos obviar que la transformación demográfica producirá un progresivo envejecimiento de la sociedad occidental, especialmente en Europa, contrariamente a lo que ocurrirá en África (hay estudios demográficos que establecen que en el año 2040 la población en África se va a multiplicar por cuatro, lo que inevitablemente nos lleva a la conclusión de que continuarán los flujos migratorios hacia Europa). La globalización e hiperconectividad son otros factores incluidos dentro de estas dinámicas intrasocietales, que harán que proliferen las redes sociales transnacionales. Otro factor a tener en cuenta es la pervivencia de estados frágiles que seguirán formando parte del mapa político mundial, especialmente en aquellas regiones menos favorecidas del planeta.

Dentro del contexto de la política nacional española, la promulgación de la Estrategia de Seguridad Nacional en 2017 trajo como consecuencia, entre otras muchas, la identificación de las amenazas y desafíos para la seguridad nacional.

Las amenazas se definen como aquellos elementos que pueden socavar la seguridad nacional. Se recogen como principales las siguientes: los conflictos armados, el terrorismo, el crimen organi-

zado, la proliferación de armas de destrucción masiva, el espionaje, las ciberamenazas, las amenazas sobre las estructuras críticas y el terrorismo yihadista. Especial mención merece esta última, por ser uno de los principales problemas de seguridad a los que se enfrenta el mundo, que ya mostró toda su brutalidad en España en agosto de 2017 y que ha provocado recientemente múltiples atentados en lugares muy diversos. En este contexto, se observa que a las amenazas tradicionales, consecuencia de las disputas entre estados por cuestiones políticas o territoriales, se sumarán las provenientes de actores no estatales, cuya influencia creciente en la seguridad internacional es consecuencia de impacto generado por la globalización. La presencia de ambas implicará un creciente y más complejo juego de intereses, donde la población siempre estará presente, bien como actor en los teatros de las operaciones o bien como audiencia, por su capacidad de emitir juicios y opiniones en el seno de las sociedades y desde sus hogares.

En cuanto a los desafíos, se determinan como aquellas circunstancias que, sin tener de por sí entidad de amenaza, pueden incrementar la vulnerabilidad, provocar situaciones de inestabilidad o la aparición de nuevas amenazas. Entre los desafíos se contemplan: la inestabilidad económica, la vulnerabilidad energética, los movimientos migratorios, las emergencias y catástrofes, las epidemias y pandemias y el cambio climático.

Las amenazas y los desafíos no existen de manera aislada sino que están interconectados. Sus efectos traspasan fronteras y se materializan con frecuencia en los denominados espacios comunes globales (ciberespacio, espacio marítimo y espacio aéreo y aeroterrestre). Ejemplos bien claros de riesgos y amenazas son el terrorismo transnacional y los ciberataques. Los potenciales adversarios, tanto actores estatales como no estatales, podrán acceder a capacidades tecnológicas de una forma barata en comparación con el coste que le supondrá a los estados el acceso a las tecnologías y técnicas necesarias para derrotarlas. Asimismo, adoptarán estrategias asimétricas o híbridas que reducirán la relevancia e importancia de las capacidades militares y favorecerán el aumento de la violencia en otros ámbitos (político, económico, tecnológico, legal, informativo, etc.). Conocido por todos es el ataque con RPAS[1]

1. Aeronave pilotada remotamente (*Remotely Piloted Aircraft*).

a refinerías saudíes con tecnologías muy baratas que afectó al 6% de la producción mundial de crudo y también la anexión de la península de Crimea por parte de Rusia. Ambos son ejemplos claros de que Occidente se va a enfrentar a partir de ahora a adversarios dispuestos a emplear todos los medios a su alcance.

En cuanto a los actores implicados, a los principales (organizaciones internacionales y estados) habrá que añadir la presencia de otro tipo de ellos que darán una mayor complejidad al escenario: estados fallidos, grupos terroristas, grupos criminales, organizaciones supranacionales gubernamentales, organizaciones no gubernamentales o alianzas constituidas *ad hoc*. Grupos extremistas, como por ejemplo Al Qaeda o el Daesh, han sido capaces de poner en jaque no solo a Oriente Medio y a África sino a todo el planeta. Además de estos actores no estatales, ciudadanos empoderados, corporaciones transnacionales, organizaciones no gubernamentales o ciudades estado, podrán ser más influyentes de lo que lo son actualmente. Por poner un ejemplo, es de esperar que las corporaciones del tipo GAFA (Google, Apple, Facebook y Amazon) tengan una gran influencia en la toma de decisiones en el futuro.

En cuanto a la situación de España, es una potencia media cuya posición geopolítica está marcada por su pertenencia a la OTAN y a la Unión Europea y por ser un país atlántico y mediterráneo que constituye la vía natural de comunicación de Europa con el Magreb y el Sahel. La Estrategia de Seguridad Nacional establece los parámetros básicos que en materia de seguridad y defensa definen el entorno geográfico al que España, por su posición estratégica, debe dirigir su atención y en el que debe centrar sus esfuerzos. Estos escenarios son: Europa, Norte de África, Oriente Medio, África Subsahariana, América Latina, América del Norte y Asia-Pacífico. Pero además de eso, el contexto actual marcado por la globalización y la proliferación de amenazas transfronterizas obliga a replantearnos el concepto de nación como área de responsabilidad exclusiva para defender nuestros intereses; es decir, que los intereses de España, como los del resto de sus países aliados y amigos, no se están jugando exclusivamente dentro de los límites del territorio nacional. A esta realidad se la conoce como frontera avanzada. Además de todo esto, las fronteras son cada vez más permeables. Constantemente, estamos recibiendo noticias de que posibles componentes del Daesh podrían llegar a

Europa como refugiados, lo que da origen a lo que se denomina retaguardia difusa. En concreto, España se enfrentará a un futuro volátil e incierto definido por la creciente velocidad del cambio y la presencia de múltiples amenazas y desafíos internos y externos. En las próximas décadas, nuestro país seguirá experimentando profundas transformaciones políticas, sociales y laborales, que afectarán ineludiblemente al Ejército de Tierra. La anticipación y la reducción de la incertidumbre proporcionarán una ventaja estratégica en el empleo de las Fuerzas Terrestres.

En el contexto de las operaciones en el entorno 2035, a los tradicionales espacios terrestre, naval y aéreo se le añadirán dos más: el cognitivo y el ciberespacial, cuya dimensión crecerá exponencialmente y de manera proporcional a los avances tecnológicos.

El cognitivo, que tiene como ámbito intangible al ser humano, buscará como objetivo fundamental ganarse a la población, puesto que su presencia será una componente constante en los conflictos del futuro. En cuanto al ciberespacial, tendremos que tener en cuenta no solo las capacidades de los sistemas de información y de telecomunicaciones (CIS)[2] sino también su enorme influencia sobre el contexto físico. Asimismo destacarán los espacios urbanos; no en vano, en el año 2035 se espera que el 65% de la población mundial viva en ciudades, y de ella el 70% en barrios marginales sin el adecuado acceso a recursos y servicios tal y como los tenemos concebidos en el mundo occidental.

Especialmente importante será saber adentrarse en los retos que supone tener que llevar a cabo operaciones en los espacios no físicos (cognitivo y ciberespacial), e incluso maniobrar en el campo de la información concurriendo de forma coordinada con la maniobra física de las unidades, con la suficiente libertad de acción. Maniobra que, probablemente, se iniciará antes del desencadenamiento de los conflictos armados, propiamente dichos. En este entorno, el modelo habitual de actuación de nuestras Fuerzas Terrestres será como fuerzas encuadradas en las organizaciones internacionales a las que pertenecemos (ONU, OTAN o UE), o en alianzas *ad hoc*. Como consecuencia de ello, las unidades terrestres verán revalorizadas su razón de ser, pero deberán evolucionar y

2. *Communications and Information Systems.*

transformarse con espíritu anticipador y no reactivo, para ser un elemento más eficaz y resolutivo en el futuro.

Muy probablemente, en el futuro, estaremos hablando de un tipo de guerra o un tipo de conflicto completamente diferente al que estamos acostumbrados. Nuestros potenciales adversarios tratarán de retarnos con medios civiles, militares y económicos en la denominada zona gris, donde el adversario pretende no cruzar los umbrales que suelen dar pie a una respuesta miliar y, en su caso, a legitimarla. Además, no podremos descartar los conflictos armados de alta intensidad, que estarán caracterizados por la tecnología, por el marco legal (el empleo de la fuerza estará sometido cada vez más a unas restricciones legales que no tendrá el adversario) y por la guerra de la información.

La guerra entendida pues como el enfrentamiento entre naciones y reconocido a nivel internacional, puede que haya perdido vigencia, puesto que apenas algo más de una veintena de ellas, pueden encuadrarse en esta concepción clásica, desde el final de la Segunda Guerra Mundial. Sin embargo, hoy en día aparecen multitud de actividades armadas o no, que siguen provocando miles de víctimas y que sin traspasar ese «umbral oficial» de la guerra, nos hacen entrar de lleno en nuevas modalidades de conflicto armado.

La naturaleza de los más recientes, tales como el desarrollado en Líbano en 2006, pasando por el más cercano de Ucrania o las acciones llevadas a cabo por el Daesh, en los que se han puesto de manifiesto nuevas tendencias a la hora de planear, dirigir y conducir las operaciones, ha llevado a numerosos autores, *think-tank* y organizaciones a emplear el término «guerra híbrida» para definir esta nueva modalidad de confrontación. Sin embargo, este concepto no es nuevo. A través de la historia, las formas y métodos «híbridos» de diferente índole han sido utilizados en diversos conflictos y batallas desde la antigüedad. Un ejemplo bien claro y cercano lo constituyen los métodos utilizados en nuestra Guerra de la Independencia para combatir la invasión napoleónica. La expresión *Hybrid Warfare*[3] se empleó por primera vez en 1998 para referirse a un modo de hacer la guerra combinando elementos de diferente naturaleza, fuerzas convencionales, no

3. Guerra híbrida.

convencionales y fuerzas especiales. Pero fue en 2005 cuando se la dotó de cierto contenido teórico en el artículo «La forma futura de hacer la guerra: el nacimiento de las guerras híbridas». En su sentido actual, el término «guerra híbrida» se hizo muy popular para referirse a los métodos empleados por Hezbolá en 2006 en su enfrentamiento con Israel. Unos años más tarde se presentó en el seno de la OTAN una iniciativa denominada *Military Contribution to Countering Hybrid Threats*[4] para adaptar la respuesta a este tipo de amenazas, que no tuvo el éxito esperado, ya que estaba demasiado focalizada hacia el escenario de insurgencia en Afganistán. Posteriormente, a partir de 2014, acontecimientos como la aparición del Daesh, la intervención de Rusia en Ucrania o la construcción de islotes artificiales de China en el Mar de China Meridional, han favorecido una evolución del término «híbrido», que se ha ido ampliando hacia otros aspectos del panorama de la seguridad internacional.

Con carácter general, podemos identificar como elemento diferencial de la guerra híbrida el empleo de cinco pilares básicos: fuerzas irregulares, acciones terroristas, crimen organizado, acciones del estado en los campos social, económico, político y diplomático, pero sin renunciar nunca al empleo de fuerzas convencionales. También destaca su capacidad para actuar de forma simultánea en los niveles estratégico, operacional y táctico; con un creciente empleo de la guerra de la información y las acciones de influencia y el ciberespacio. Y buscando tanto efectos físicos, como psicológicos e incluso ideológicos.

A modo de conclusión, las principales características del conflicto armado futuro pueden ser: la rapidez en la toma de decisiones, la mayor letalidad de las acciones violentas, el empleo del ciberespacio y el dominio de la información como espacios esenciales para alcanzar los objetivos, acciones en el ámbito cognitivo, presencia permanente de población, tecnológicamente avanzado, campos de batalla profundos y sensorizados, presencia de multitud de actores y limitaciones en el empleo de la fuerza letal por nuestra parte, pero no por parte del adversario.

El entorno operativo estratégico va a ser creciente en complejidad. El concepto de seguridad va a trascender más allá del

4. Contribución militar para contrarrestar las amenazas híbridas.

ámbito militar y la seguridad se va a garantizar no solo actuando en nuestras fronteras sino también influyendo mediante las acciones derivadas de los conceptos de frontera avanzada y retaguardia difusa. Los riesgos y amenazas serán difusos y cambiantes. En la tipología de los conflictos aparecerán las ya nombradas amenazas híbridas.

En los escenarios futuros, las fuerzas terrestres deberán reaccionar más rápido, ser más modulares, tecnológicas, autónomas e interoperables con todos los socios o aliados con los que desempeñen sus misiones, imprimiendo así un nuevo carácter a sus organizaciones operativas. Su organización, sus procedimientos, y sus medios, deberán adaptarse a los nuevos retos, aprovechando todas las oportunidades que ofrecen las nuevas herramientas, pero sin olvidar que el factor humano seguirá siendo el único facilitador de la transformación de los ejércitos y se le exigirán mayores cualidades y preparación.

Finalmente, la tecnología será muy protagonista en los retos a los que se enfrentarán las fuerzas terrestres y formará parte de la incertidumbre en la evolución del entorno, por lo que serán fundamentales la investigación, la experimentación y el seguimiento de esta en estrecho contacto con la industria de defensa y el mundo universitario, todo ello para hacer un adecuado uso de aquellas tecnologías que supongan una mejora en las capacidades militares, evitando la sorpresa y todo ello, con la perfecta integración del factor humano, que seguirá siendo del único elemento fundamental capaz de actuar en cualquier espectro del conflicto, con capacidad de inclinar la balanza a nuestro favor.

Retos y necesidades del Ejército de Tierra para operar en los nuevos escenarios

José Manuel de la Esperanza y Martín-Pinillos
General de Brigada de la División de Planes del Estado Mayor del Ejército de Tierra

El panorama estratégico y el entorno operativo van a definir las fuerzas y capacidades necesarias para afrontar los retos que se van a plantear en el futuro. En estos escenarios futuros las fuerzas terrestres deberán ser capaces de llevar a cabo diferentes tipos de operaciones, tales como acciones de estabilización, ofensivas, defensivas y de apoyo a autoridades civiles. Hemos visto que uno de los factores más determinantes del panorama global es el vertiginoso incremento y difusión de los avances tecnológicos que ya incorporan nuestros adversarios, lo que hace preciso incorporarlos a nuestras fuerzas. El Ejército de Tierra afronta este reto mediante la adaptación y la innovación a través de un proceso de incorporación de tecnologías que proporcionen mayores y mejores capacidades, mayor flexibilidad en el empleo y mayor polivalencia para llevar acabo todo tipo de operaciones, quizás incluso con una necesidad menor de personal.

El empleo de las Fuerzas Armadas se materializará mediante la actuación de una fuerza conjunta que deberá adecuar sus capacidades y preparación para contribuir a combatir las amenazas. Podemos afirmar que las fuerzas terrestres son las más indicadas para aportar determinadas capacidades claves al empleo conjunto de las Fuerzas Armadas, toda vez que tienen un abanico de capacidades esenciales que garantizan la disuasión, la respuesta escalonada para gestión de cualquier crisis, la ocupación del terreno y el apoyo a autoridades civiles.

La Fuerza 35 es la respuesta eficaz de adaptación y de innovación militar del Ejército de Tierra ante los nuevos retos. El objetivo de esta iniciativa es conseguir una fuerza terrestre moderna que incorpore tecnologías de última generación para ofrecer a nuestras fuerzas la ventaja operativa que necesitan en el campo de batalla. La iniciativa incluye un nuevo modelo para nuestras

brigadas (la Brigada 2035) pero es bastante más, ya que es una transformación que afecta a toda la fuerza terrestre. Esta transformación implica una modificación en el empleo de la fuerza y, probablemente, un cambio de mentalidad en el Ejército de Tierra.

Para identificar las características y capacidades genéricas de las fuerzas terrestres necesarias para desarrollar el proyecto de Fuerza 35 se han analizado cuatro entornos de actuación que permiten definir unas fuerzas capaces de actuar en todos ellos: apoyo a autoridades civiles, áreas urbanizadas, campo de batalla no lineal y enfrentamiento de alta intensidad. Estos cuatro entornos de actuación se han analizado en estado puro para definir los conceptos y las capacidades necesarias en cada uno de ellos, pero la realidad de las operaciones puede hacer que se presenten de manera simultánea. De hecho, la principal conclusión de este estudio es que el escenario más exigente y peligroso sería, probablemente, el de un combate de alta intensidad con presencia de población civil en zonas urbanizadas con espacios de batalla no lineales.

Este cambio responde a varios factores esenciales: la variación del entorno en el que se desarrollan las operaciones militares (el conocido como entorno VUCA[1]), la coherencia con los objetivos estratégicos de la Directiva de Planeamiento Militar, la existencia de tecnologías disruptivas que ya incorpora el adversario, la posibilidad de cooperar con la industria y la universidad y la necesidad de la interoperabilidad y del alineamiento con nuestros socios y aliados, algunos de los cuales ya están desarrollando programas e iniciativas similares (por ejemplo, el Reino Unido con la iniciativa Agile Warrior, Francia con el programa Scorpion, los Estados Unidos con la Tercera Estrategia de Compensación e Italia con el plan Prospetta).

Los pilares en los que se basará el cambio son los conceptos, la tecnología y la organización. En cuanto a los conceptos, se ha de buscar una mentalidad expedicionaria, una mayor velocidad en las operaciones y una actuación simultánea en los dominios físico, cibernético y cognitivo. Respecto a la tecnología, debemos incorporar tecnologías avanzadas y disruptivas que permitan

1. Volátil, incierto, complejo y ambiguo (*Volatility, Uncertainty, Complexity and Ambiguity).*

afrontar los cambios identificados y que proporcionen la ventaja operativa a la fuerza. Los cambios en la organización deberán permitir una reducción de personal y de la huella logística al tiempo que deberán mejorar la interoperabilidad y facilitar la consecución de unas estructuras más polivalentes, buscando la máxima similitud posible entre la estructura orgánica y la operativa.

Dentro de esta nueva Fuerza 35, la Brigada 2035 será el componente esencial y la unidad de referencia. Es la unidad básica para la generación de la fuerza, capaz de cumplir con las misiones asignadas en los posibles entornos operativos. Tiene una estructura orgánica con carácter interarmas que integra todas las funciones de combate a nivel táctico. Para ello, la brigada, como sistema de combate integral, contará con unidades orgánicas de maniobra, mando y control y telecomunicaciones, reconocimiento, inteligencia, apoyos de fuego, defensa antiaérea, maniobra de la información, movilidad y contramovilidad, protección y apoyo logístico. Es importante subrayar que todas las brigadas del Ejército de Tierra no serán iguales, ya que se mantendrá la orgánica de brigadas pesadas con medios cadena, brigadas medias con medios rueda blindados (fundamentalmente el conocido 8x8 Dragón) y brigadas ligeras con medios rueda ligeros y protegidos. Pero todas las brigadas incorporarán el modelo Brigada 2035 en cuanto a innovación tecnológica y nueva mentalidad de organización y de liderazgo.

Las cifras de la Brigada 2035, de acuerdo con los estudios que estamos llevando a cabo, se estiman en un componente humano de alrededor de dos mil ochocientos combatientes, unas novecientas plataformas y una autonomía de combate estimada en siete días. Como elementos de maniobra, la Brigada 2035 estará integrada por tres grupos de combate que dispondrán más o menos de unas cien plataformas de todo tipo. Cada grupo de combate estará integrado a su vez por tres subgrupos de combate compuesto cada uno de ellos por unos cien combatientes y dieciséis plataformas. El resto de apoyos se integrarán en un núcleo de tropas de brigada.

Pero la Fuerza 35 es mucho más que la Brigada 2035. Evidentemente, la transformación afectará a todas las unidades de las fuerzas terrestres. Inicialmente se comenzará por transformar la unidad de referencia pero el proceso se extenderá simultáneamente al resto de capacidades de apoyo al combate y apoyo logís-

tico encuadrados en los escalones superiores a brigada, actuando sobre las capacidades de operaciones especiales, defensa NBQ[2], logística, inteligencia, CIS, ingenieros, defensa antiaérea, fuegos y aviación de ejército.

Pero nos encontramos con el nuevo paradigma de la obtención. Con el sistema actual de adquisición por sistemas parciales las brigadas nunca tienen sus capacidades plenamente operativas, siendo fácil que algunas estén ya obsoletas mientras que otras todavía se estén generando, lo que reduce su operatividad. Por ello, la ambición del Ejército de Tierra es que la brigada sea diseñada, desarrollada y puesta en servicio de forma simultánea y completa. A este respecto se suele poner el ejemplo de la fragata: cuando se bota un navío de este tipo para la Armada, el barco cuenta con la dotación y equipamiento al completo para cumplir todos los cometidos para los que fue diseñado. Es mucho más difícil hacer esto con una brigada pero debemos tender a un sistema que sea parecido. Para conseguir este objetivo resulta clave conseguir la máxima implicación de la industria de defensa. Son también necesarios unos presupuestos estables y suficientes que permitan trabajar con la necesaria anticipación y previsión y es necesario acometer los programas necesarios de una forma completa en un nuevo paradigma de obtención.

Para alcanzar el estado final deseado en 2035 será preciso llevar a cabo de manera simultánea unos procesos de desarrollo conceptual, de experimentación y de implementación de todas esas capacidades que se han identificado. Se han definido tres objetivos parciales, alineados con los ciclos de planeamiento de capacidades del Ministerio de Defensa: 2024, 2030 y 2035. En cada hito temporal tenemos la previsión de ser capaces de transformar, o mejor dicho, de generar dos brigadas. Lo importante es destacar que en el año 2024 alcanzaremos una fuerza posible, que combinará programas que ya están en curso con nuevos desarrollos y adquisiciones. Para el año 2030 prevemos disponer de lo que llamamos la fuerza avanzada, que incorporará destacados avances tecnológicos compaginados con programas que están ahora en curso y modernizaciones de sistemas. Finalmente, en el año 2035 pretendemos alcanzar la fuerza de ventaja, que es el estado final

2. Nuclear, biológico y químico.

deseado, una fuerza tecnológicamente avanzada que proporcione una verdadera ventaja militar.

A continuación analizaré brevemente la influencia y las posibilidades que pueden tener los avances tecnológicos (tales como la inteligencia artificial, digitalización, fabricación aditiva, radar evolutivo, sensorización-hiperconectividad, *big data*, energías alternativas, miniaturización, robótica, drones, etc.) en las áreas de la fuerza terrestre.

En cuanto a capacidades de mando, los focos de la brigada tienen que ser los terminales satélites portátiles, la red-radio de combate de banda ancha, el sistema de integración del combatiente a pie, los protocolos de interoperabilidad entre sistemas de información y la seguridad de las comunicaciones y de la propia información. Hay que intentar conectar el nivel brigada con el combatiente aislado a través del intercambio de voz, datos y vídeo y se debe garantizar la difusión y el uso compartido de la misma imagen operativa común (COP)[3] de manera única e interoperable, con el ancho de banda adecuado y con difíciles soluciones técnicas (mucho más en combate).

En cuanto a inteligencia, los focos para la brigada son los sistemas pilotados remotamente (RPAS o drones), las plataformas de observación aérea, los robots terrestres (tanto de superficie como subterráneos) y los sistemas de inteligencia artificial que permitan la gestión de información e identificación.

En cuanto a maniobra, el desafío de la brigada es disponer de una flota de plataformas de combate, cadenas y ruedas en el estado del arte tecnológico (superando los blindados medios sobre ruedas sobre los que hemos combatido estos últimos treinta años) complementada con medios blindados de zapadores y medios autónomos y robotizados que nos doten de libertad de acción, completado todo ello con un combatiente individual potenciado física y cognitivamente.

En cuanto a capacidad de fuegos, las mejoras apuntan a proporcionar mayor alcance y precisión. Además, la aplicación de tecnologías debe permitir acceder a la capacidad de fuegos en red, de tal modo que todos los orígenes de fuegos estén conectados. Las municiones guiadas e inteligentes de elevada precisión y

3. *Common Operating Picture.*

las de alcance extendido permitirán incrementar la eficacia de la fuerza y reducir su huella logística.

En cuanto a capacidades de protección, el desafío es conseguir la capacidad de protección en forma de burbuja de tres dimensiones (burbuja 3D), construida sobre todo con medios de defensa antiaérea en red, guerra electrónica, enmascaramiento y defensa NBQ. Los RPAS constituyen una amenaza constante en el campo de batalla y exigen una adecuada defensa coordinada con la defensa antiaérea. En este ámbito, las nuevas tecnologías deben permitir una adecuada detección e identificación de los aparatos y su neutralización mediante capacidades convencionales, electromagnéticas o armas de energía dirigidas, como puede ser el láser.

En cuanto al apoyo logístico, el desafío está en reducir la huella logística y energética a través de aplicaciones que faciliten la telemecánica, el autodiagnóstico, la eficiencia energética, la captación de recursos locales, la autogeneración de energía, la incorporación de sistemas autónomos de abastecimiento y transporte robotizados, la adquisición de material de campamento y vestuario de última generación, la telemedicina y, por supuesto, la fabricación aditiva.

Respecto a las capacidades de helicópteros, prevemos una progresión a partir de las familias que ahora mismo tenemos (Tigre, Chinook, NH90 y Cougar). Los helicópteros de combate deben incrementar sus capacidades de integración en la maniobra aeroterrestre (mediante adecuados medios CIS y la hiperconectividad) y sus capacidades de protección. Los helicópteros pesados de transporte se han mostrado especialmente válidos en ambientes urbanos y esa utilización tiende a ir a más, sobre todo porque facilita una concentración rápida de efectivos contra las amenazas híbridas.

En operaciones especiales las claves están en una mayor integración entre fuerzas de operaciones especiales y fuerzas convencionales, en su empleo rápido, eficaz y, sobre todo, discreto y en el fortalecimiento e impulso del desarrollo de capacidades de inteligencia, en especial la inteligencia procedente de fuentes humanas (para lo que se necesita personal capaz de obtener información de la población local, que domine el idioma, que tenga el mismo aspecto y que esté integrado culturalmente).

No creo que sea un cambio cultural sino más bien un cambio de mentalidad. Pero es bien cierto que, junto a la tecnología, el

otro gran pilar de la Fuerza 35 es el militar combatiente, principal elemento de la fuerza. El militar debe estar preparado para el combate y para actuar de forma más autónoma y con mejores medios, lo que solo será posible con una mejor formación y preparación (de lo que se encarga precisamente el MADOC) y con el ejercicio de los valores de liderazgo y del mando orientado a la misión (*mission command*), propósito que propugna la Fuerza 35 (dotar de iniciativa al subordinado). En resumen, la transformación de la fuerza actual hacia el concepto Fuerza 35 será posible si se siguen de manera adecuada los siguientes pasos: progresiva definición de conceptos y necesidades, investigación, experimentación, desarrollo industrial y obtención. Todo ello para alcanzar el objetivo final: la fuerza de ventaja.

Como ideas fuerza de todo lo expuesto se podrían extraer las siguientes: las fuerzas terrestres seguirán siendo un elemento fundamental, toda vez que tienen la capacidad de respuesta en la totalidad del espectro del conflicto y de llevar a cabo maniobras en todos los dominios; la gran influencia de los avances tecnológicos en el combate actual; la Fuerza 35 estará basada en la incorporación de tecnologías en un proceso continuo y progresivo en el horizonte 2035, siendo la brigada la unidad de referencia; será necesario definir y consolidar un modelo de adquisición que considere a la brigada como un sistema de combate integral, con las dificultades que ello conlleva; será necesaria la participación de la industria de defensa y de la universidad como guardianes del conocimiento; se requerirán recursos económicos estables y suficientes; y por último y no menos importante, el combatiente seguirá siendo el centro de gravedad de la fuerza y tendrá que estar suficiente y convenientemente instruido y adaptado a todos estos múltiples cambios y retos a afrontar.

Retos tecnológicos en el ámbito de la Universidad

Enrique Herrera Viedma
Vicerrector de Investigación y Transferencia de la Universidad de Granada

La universidad española está en condiciones de colaborar con las fuerzas de seguridad y defensa en el diseño de la futura Fuerza 35. Ha sido capaz de remontar y de mantenerse a flote a pesar de la crisis económica que le está afectando desde 2011. Las políticas que se están intentando desarrollar permiten albergar esperanzas para poder contribuir al desarrollo español en temas de investigación y defensa y en cualquier otro reto tecnológico que se le plantee. Los tres pilares fundamentales de la universidad son la docencia (transmisión del conocimiento), la investigación (generación del conocimiento) y la transferencia (aplicación del conocimiento). Centrándome en los dos últimos pilares pretendo mostrar dónde estamos, qué políticas estamos implementando y hacia dónde queremos ir.

La Universidad de Granada tiene en torno a unos sesenta mil estudiantes. Como consecuencia de la segregación de las Universidades de Almería y de Jaén sufrió una pérdida de alumnos nacionales pero ha sabido trabajar bien el aspecto internacional, con lo que ha conseguido mantener su cuota de alumnado. Tiene un potencial de tres mil quinientos investigadores trabajando activamente en muchas áreas del saber, organizados en quinientos veintisiete grupos de investigación que trabajan en mil quinientas sesenta y cuatro líneas diferentes. Además tiene en torno a mil quinientos efectivos que apoyan y soportan toda esa investigación. Dispone también de ciento treinta unidades de apoyo a la I+D compuestas por técnicos de laboratorio que contribuyen a fortalecer las investigaciones. El presupuesto anual para hacer frente a todas sus actividades y servicios ronda los cuatrocientos millones de euros.

Todo este potencial se distribuye en diferentes infraestructuras: cuatro escuelas, veintidós facultades, ciento veintitrés departamentos de docencia e investigación, cinco centros de

investigación, quince institutos de investigación, un centro asociado de investigación, un Centro de Instrumentación Científica (CIC) que da soporte a la mayoría de investigación que se desarrolla en la Universidad de Granada, un Centro de Investigación TIC[1] (CITIC), un Centro de Empresas TIC (CETIC) y un Parque Tecnológico de la Salud (PTS), centro peculiar en el coexisten grupos de investigación con el hospital y con empresas del sector privado que están colaborando para investigar en temas sanitarios (la Universidad de Granada es la única en Andalucía que cuenta con esta estructura PTS, siendo uno de sus valores y fortaleza).

Una característica muy relevante de la Universidad de Granada es su carácter generalista. Las humanidades y las sociales fueron las fortalezas principales desde su inicio, pero a pesar del aislamiento geográfico que ha sufrido como consecuencia de no tener buenos medios de transporte ha ido avanzando en otras disciplinas (ingenierías, arquitectura, informática, etc.). Aun siendo generalista hoy por hoy se puede constatar que sigue manteniendo posiciones destacadas en temas humanísticos y sociales y que empieza a despuntar también en temas relacionados con las TIC, con las ingenierías, con las ciencias físicas, etc. Es muy importante tener esto en cuenta cuando se comparan universidades españolas de perfil generalista con universidades de otros países que no tienen esta característica sino que están más centradas en temas TIC, son más específicas y no trabajan otras áreas del saber. A este respecto cabe decir que tanto desde el ámbito académico como desde el mundo empresarial se está poniendo de manifiesto la importancia de compaginar la formación técnica con la formación social y humanística.

La Universidad de Granada suele aparecer en puestos cabeceros en los *ranking* que evalúan la cualificación de universidades, pero para nosotros es fundamental hacerlo de manera destacada en el Shanghai Ranking, el cual establece un estándar internacional para evaluar la calidad de una universidad con una forma de clasificar que está muy centrada en temas de investigación sin dejar de lado el tema de la docencia. En este *ranking* la Universidad de Granada aparece siempre entre las cinco mejores de España (en el año 2017 se encontraba en el *top* 3, en 2018 en el

1. Tecnologías de la Información y de la Comunicación.

top 4 y en el año 2019 le corresponde estar en el *top* 5 junto con otras universidades españolas de relevancia, como son algunas de Barcelona, Madrid y Valencia). A nivel mundial, la Universidad de Granada está entre las trescientas mejores de entre las diecisiete mil universidades que se evalúan en esta clasificación. A pesar de que España ha venido sufriendo una especial penuria económica en los últimos tiempos, a partir del año 2014 siguió manteniendo el tipo e incluso subió y se mantuvo en este nivel. Teniendo en cuenta el limitado presupuesto de las universidades españolas y su carácter generalista, aparecer año tras año entre las trescientas mejores es una tarea muy complicada pero viene a demostrar que no todo depende del dinero sino que también importa el trabajo, el esfuerzo y la capacitación del personal docente e investigador. El Shanghai Ranking deja claro que la Universidad de Granada tiene potencial suficiente para poder realizar un trabajo docente y una investigación de calidad. Si dispusiera de más recursos económicos y de más apoyos, a buen seguro estaría más arriba en la clasificación, sin dejar nuca de lado su perfil generalista.

En determinadas áreas la Universidad de Granada ha figurado y/o figura entre las mejores del mundo. Por ejemplo, en temas relacionados con nutrición y en *computer science & engineering*[2] está apareciendo en los últimos cinco años en el *top* 100 mundial de universidades con mejor investigación y mejores resultados, de acuerdo al Shangai Ranking. También aparece en puestos destacados en otros temas, como en ciencias de la documentación, matemáticas, geología y salud.

En cuanto a producción científica se refiere, la Universidad de Granada aparece frecuentemente capitaneando de forma consistente y consolidada las comparativas con otras universidades españolas en determinadas áreas. En las últimas clasificaciones ha venido ocupando posiciones destacadas en treinta y seis disciplinas científicas, sociales, de psicología y de derecho.

Hace unos años, Times Higher Education (THE)[3] hizo un estudio sobre cuáles son los países que están más activos en producción científica relacionada con inteligencia artificial. Dicho

2. Ingeniería y ciencia de la computación.

3. Revista semanal que informa específicamente de noticias y asuntos relacionados con educación superior. En el Reino Unido es la publicación principal en su campo.

estudio mostró un cambio en el liderazgo en este ámbito (China ha sobrepasado a los Estados Unidos). También indicó que España se encontraba en séptima posición. Con posterioridad se hizo un estudio más pormenorizado y más exhaustivo que permitió conocer cuáles eran las universidades que más están contribuyendo. Naturalmente, en los puestos de cabeza figuraban universidades estadounidenses. También universidades de Singapur. Pero lo más importante para nosotros es que la Universidad de Granada aparecía en el cuarto puesto. Cuando se habla de inteligencia artificial se está hablando de muchos grupos de investigación que trabajan en temas relacionados con drones, ciberseguridad, *deep learning*, toma de decisiones, *smart city*, 5G y otros temas relacionados con todas las tecnologías disruptivas que están contribuyendo al desarrollo de la sociedad.

En cuanto a proyectos de investigación nacionales, la Universidad de Granada ha ido manteniendo un número de proyectos y una financiación razonable a pesar de las penurias económicas. Los contratos de la Oficina de Transferencia de Resultados e Investigación (OTRI) también se han ido incrementando a pesar de esa escasez de recursos económicos (este incremento no ha sido solamente en número de contratos sino también en dinero facturado).

En temas de patentes, a través de las cuales se materializa la transferencia a la sociedad de los resultados de la investigación, en el año 2018 la Universidad de Granada ocupó el quinto lugar en solicitudes de patentes nacionales y el tercer lugar en patentes internacionales (se solicitaron doscientas cincuenta y se concedieron ciento noventa y ocho). Por áreas, destacan las relacionadas con temas de salud, con las TIC y con la ciencia.

En cuanto a la creación de empresas de base tecnológica, también se hace una labor ingente: se han creado noventa y cuatro, de las cuales un 69% siguen activas a día de hoy.

No se debe olvidar que en el ADN de la Universidad de Granada está la apuesta por la investigación de calidad. Y esta investigación de calidad se consigue cuando se indaga sobre lo que están haciendo otras universidades y sobre lo que se investiga en el resto del mundo. Las variables fundamentales de las que depende una investigación de calidad son tres. Una de ellas es la multidisciplinaridad. Hoy día no se puede trabajar aislado en un laboratorio sin contar con los demás, y en eso la Universidad de Granada tiene muchas oportunidades, pues es una universidad

generalista donde pueden trabajar conjuntamente y colaborar hacia un fin común investigadores con distinta mentalidad y con distinta formación. Otra variable es la excelencia: es fundamental trabajar en temas y retos frontera sin conformarse con ámbitos cómodos y confortables. Y por último, es muy importante la internacionalidad, que se debe afrontar desde el liderazgo y desde el protagonismo.

Evidentemente, para incorporar estas tres variables a la investigación hacen falta unos recursos humanos y económicos nada desdeñables. Habida cuenta de los escasos recursos con los que se cuenta en España para desarrollar tareas de investigación, es necesario implementar políticas que permitan incrementar el acceso a proyectos europeos tales como el programa Horizonte 2020 y el Consejo Europeo de Investigación (ERC)[4], el cual concede proyectos de dos millones de euros a individuos por desarrollar investigación de conocimiento de frontera. Para potenciar esta línea de actuación la Universidad de Granada ha diseñado un programa de intensificación de la investigación de excelencia: se ayuda a los investigadores a que focalicen su actividad en áreas que permitan solicitar proyectos ERC y una vez conseguidos se les presta la ayuda necesaria para que mantengan el liderazgo en su desarrollo. De este modo se les libera de tareas ligadas a temas burocráticos y temas de docencia.

También se ha incorporado un plan de captación de talento de alto nivel que se llama Programa Athenea. Si bien los emolumentos que ofrece la Universidad de Granada son los mismos que ofrecen el resto de universidades españolas, este programa ofrece la oportunidad de acceder a salarios de rango europeo, que muchas veces superan a los nacionales en un 40%-50%. En los últimos cuatro años este programa ha permitido captar veinte investigadores de alto nivel, muchos de ellos nacidos en España. Todos ellos traen consigo nuevas líneas de investigación a desarrollar en la Universidad de Granada durante tres años con la obligación de solicitar un proyecto ERC. Para incrementar la captación de talento también se están utilizando programas nacionales tales como el Ramón y Cajal, el Juan de la Cierva y el programa Marie Curie. Paralelamente la Universidad de Granada está trabajando en la

4. *European Research Council.*

creación de un plan de estabilización que permita consolidar una plaza en esta Universidad a los investigadores que terminan sus proyectos Ramón y Cajal o Juan de la Cierva.

Se ha incrementado la colaboración con empresas y se ha dotado a la Universidad de un programa de Cátedras Empresa-Universidad con la intención de formar estudiantes alineados con los requerimientos de la empresa. Mediante este programa se crean foros de intercambio de opiniones y se transmiten ideas a universitarios y empresarios de cara a la solicitud o diseño de proyectos futuros. Cabe decir que está teniendo bastante éxito y muchas firmas se están acogiendo a él para hacer un primer acercamiento a grupos de investigación de nuestra Universidad.

Además se ha trabajado activamente para incrementar el liderazgo nacional, lo que para mí constituye el programa estrella de la Universidad de Granada. Con las ideas de internacionalidad, excelencia y trabajo multidisciplinar hemos desarrollado un programa de excelencia que permite crear grupos que colaboran activamente para intentar ser acreditados a nivel nacional como Centros de Excelencia similares al Severo Ochoa-María Maeztu que se ha fraguado en el Ministerio de Ciencia desde el año 2011. Si esto se consigue no solo se accede a un presupuesto que oscila entre dos y cuatro millones de euros sino que también se incrementan las posibilidades de captar más talento. La mayoría de los Centros de Excelencia se localizan en la mitad norte de España, principalmente en Cataluña y Madrid. Andalucía está carente de ellos, por lo que estamos trabajando para liderar un movimiento que permita crear Centros de Excelencia con nuestras capacidades. Con esta política, hasta el momento se han conseguido establecer diecinueve Unidades de Excelencia en todas las áreas que tenemos del saber. En humanidades se han establecido cinco, entre las que destaca Ciencia en la Alhambra, unidad en la que colaboran equipos multidisciplinares de matemáticas, biología, patrimonio, historia e informática, entre otros, para desarrollar nuevas investigaciones en torno al monumento por excelencia que tenemos en Granada. Hay grupos de ciencias sociales-económicas orientados a la sociedad digital, a la seguridad y protección de derechos y al turismo. Hay cinco unidades en salud y otras tantas en educación (física, química y matemáticas, nanotecnología y uno muy importante de ciencia de datos e inteligencia artificial, que se ha gestado entre las Universidades de Granada, Jaén y de Córdoba, consiguiendo así

una especie de movimiento autonómico). El objetivo para el que se está trabajando es llegar a convertir muchas de estas unidades en centros de referencia de investigación a nivel nacional.

Además de todo esto, la Universidad de Granada está liderando tres importantes proyectos de investigación. El primero es un proyecto encuadrado en la Alianza Europea ARQUS para el que se presentaron cincuenta y cuatro candidaturas y se identificaron diecisiete. Cuenta con un presupuesto inicial de cinco millones, que a buen seguro se irá incrementando a medida que cuaje su actividad, lo que permitirá a la Universidad de Granada convertirse en un referente internacional. Otro proyecto que la Universidad de Granada está liderando es el de implementación de un acelerador de partículas IFMIF-DONES en la provincia de Granada, que tiene como objetivo sentar las bases para la construcción en el futuro de una central nuclear por fusión y no por fisión, con lo que se conseguirá un menor impacto climático y medioambiental sin menoscabo del potencial de generación de energía. Se estima que el presupuesto inicial de este proyecto puede rondar los seiscientos millones de euros. En caso de llevarse a cabo, la Universidad de Granada se ha posicionado como la universidad que lo capitanearía. De momento ya se ha conseguido un proyecto de la Unión Europea dotado con cuatro millones de euros orientado hacia las actividades preparatorias desde una perspectiva legal, financiera y de madurez tecnológica. Además, la Junta de Andalucía acaba de presupuestar doce millones de euros para empezar a desarrollar cuatro laboratorios en la Universidad de Granada ligados a este proyecto y el Ministerio tiene previsto aportar otros dieciséis millones de euros para seguir avanzando. Por último, otro proyecto que se está liderando es el LifeWatch ERIC, relacionado con el cambio climático, dotado inicialmente con siete millones de euros. Su objetivo es crear un observatorio de *big data* basado en inteligencia artificial para la predicción del cambio climático aprovechando las especiales condiciones que ofrece Sierra Nevada. Lo que se pretende es estudiar cómo mejorar la calidad de vida de todos los pueblos cercanos a esta sierra y a raíz de ello crear patrones de comportamiento de adaptación que puedan ser de aplicación en otras zonas de Europa.

Con todo lo expuesto queda claro que la Universidad de Granada tiene potencial más que suficiente para colaborar en el futuro diseño de la Fuerza 35.

Retos tecnológicos en el ámbito empresarial

Jesús Alonso Martín
Director de Desarrollo de Negocio de Ingeniería de Sistemas para la Defensa de España

Ingeniería de Sistemas para la Defensa de España (ISDEFE) fue creada por el Ministerio de Defensa en el año 1985 con el objetivo de apoyar técnicamente la definición de los programas del Ministerio. Esta empresa ha estado ligada desde sus orígenes a la tecnología y a la innovación. En la declaración del Consejo de Ministros en la que se anunció su creación consta una frase que refleja fielmente el espíritu de la compañía: «La complejidad, sofisticación y rapidísima evolución de los sistemas de armas exigen al Ministerio de Defensa la posibilidad de tener a su servicio un personal de altísima cualificación tecnológica capaz de abordar las tareas de definir técnicamente las necesidades que, derivadas del Plan Estratégico Conjunto, definan desde el punto de vista operativo los Estados Mayores». Esta frase continúa teniendo pleno valor en la actualidad, tanto por las necesidades de los ejércitos como por la función que se desarrolla.

La innovación es consustancial a nuestra actividad. Nuestra función es conocer y anticipar las tecnologías para poder incorporarlas a los nuevos programas de defensa. Ante el ritmo actual del desarrollo tecnológico se puede afirmar que la importancia de nuestra función es mayor ahora que hace treinta y cinco años. Cuando se habla de innovación y de organizaciones innovadoras siempre se piensa en los sectores tecnológicos, financieros, en sectores y empresas de diferentes sectores productivos, etc. Personalmente pienso que los ejércitos son las organizaciones más innovadoras que existen. Las amenazas que afrontan cambian constantemente, cada operación es distinta de la anterior, necesitan nuevos materiales y sistemas que hay que desarrollar, lo que a su vez conlleva nuevas formas de organizarse, nueva doctrina y nuevas formas de actuación que obligan a un proceso de reinven-

ción constante. Esto no quiere decir que ni Google ni Amazon sean innovadoras, que lo son, pero no lo son más que los ejércitos, los cuales llevan años y siglos de evolución para desarrollar una misión y estar en todo momento en la punta de lanza de la tecnología. Porque sin tecnología no hay ejércitos.

En ISDEFE no desarrollamos las tecnologías. Esa función la hacen las universidades, las empresas, los centros de investigación, etc. Nuestra función es apoyar y acompañar al Ministerio de Defensa, que será el usuario de esas tecnologías, a través de un proceso integral de análisis, asesoramiento y recomendación. Fundamentalmente trabajamos en cuatro aspectos: identificar y conocer qué tecnologías nos esperan en el futuro; anticipar la repercusión que pueden tener esas tecnologías tanto en la defensa y la seguridad cómo en el resto de la Administración; definir, a través de un análisis 360º, cómo se utilizarán esas tecnologías, cuáles serán las implicaciones, descubrir nuevas utilidades y nuevas conexiones con otras tecnologías; y por último, apoyar su implantación y ayudar a la superación de los retos que se planteen en su utilización.

Para desarrollar esta función tenemos que generar nuestro propio conocimiento. Ese conocimiento no se puede comprar sino que lo tenemos que crear, y para eso en ISDEFE hemos establecido un sistema de I+D+i que se articula fundamentalmente en tres ejes. El primer eje es el de proyectos de investigación científica y desarrollo, los cuales pueden ser externos (financiados mediante fondos europeos u otro tipo de financiación), internos (financiados íntegramente con fondos de la compañía y basados fundamentalmente en un programa de captación y gestión de ideas) y bilaterales con otros organismos. El segundo eje es la Red Horizontes, vehículo a través del cual articulamos la innovación en los ámbitos estratégicos de la compañía y mediante el cual adquirimos la capacidad de anticiparnos a las oportunidades y retos a los que debe enfrentarse la Administración, desarrollando las ideas y planteando soluciones innovadoras. El tercer y último eje es la promoción de la innovación, que es un sistema a través del que pretendemos desarrollar la cultura global de innovación en toda la plantilla de ISDEFE.

Así pues, la innovación en ISDEFE se articula básicamente a través de la Red Horizontes. Esta red identifica y aprovecha las fuentes de conocimiento que existen en el ecosistema de innova-

ción que rodea nuestra compañía, establece un abanico de líneas de actividad enfocadas tanto a nuestra plantilla como a Defensa o al resto de organismos de la administración para la que trabajamos y pone a disposición de la organización herramientas para fomentar la cultura corporativa e innovadora de la plantilla. Las fuentes con las que nos nutrimos y trabajamos proceden principalmente del conocimiento académico conseguido por los grupos de investigación de las universidades. Tenemos seis cátedras con diferentes universidades (españolas y alguna extranjera) y otros organismos (el Centro Superior de Estudio para la Defensa Nacional y la Real Academia de Ingeniería, entre otros). Otra de nuestras fuentes es el conocimiento interno que proporcionan los empleados de nuestra compañía, obtenido con el paso de los años mediante su formación especializada y el trabajo que han desarrollado para la Administración. También son muy importantes las fuentes de conocimiento que proceden de los organismos públicos para los que trabajamos (administraciones y organismos nacionales y europeos), que pueden residir en su personal o estar plasmadas en fuentes documentales tales como la Estrategia de Tecnología e Innovación para la Defensa, el documento de Entorno Operativo 2035 del Ministerio de Defensa o el Plan Director de Sistemas Espaciales, entre otros. Y por último, otras fuentes de conocimiento son las fuentes abiertas, información pública de acceso libre o bajo subscripción que es de alto interés para nuestra compañía y sus áreas de actividad.

Las actividades que desarrolla la Red Horizontes se articulan en torno a cinco líneas principales de actuación. La primera de ellas es la vigilancia y prospectiva tecnológica, que consiste en poner en marcha un proceso organizado capaz de captar, seleccionar y analizar las comunicaciones y la información sobre ciencia y tecnología que ayudan a la toma de decisiones. La segunda son los estudios especializados en distintos ámbitos de interés tecnológico y de gestión. La tercera es la difusión y explotación de los resultados, tanto internos como externos. La cuarta es el establecimiento de una red de alianzas y colaboraciones para reforzar las relaciones con otras entidades y organismos con perfil innovador y de interés común. Y la quinta línea, una de las más importantes, es la captación del talento, esto es, la necesidad de identificar el talento en las etapas tempranas para poder atraer a ISDEFE a los perfiles altamente cualificados en los ámbitos en los que trabajamos.

La Red Horizontes funciona con una serie de herramientas. La primera herramienta son los observatorios, nodos de la red a través de los cuales se desarrollan las actividades de prospectiva y análisis metodológico y tecnológico (son las cátedras ya mencionadas). Estos observatorios están dirigidos por una persona de ISDEFE y por un catedrático de universidad. Otra de las herramientas son las comunidades de conocimiento, grupos multidisciplinares formados por personal de ISDEFE para que puedan compartir su experiencia y conocimiento en un marco colaborativo. Una tercera herramienta la constituyen los grupos de reflexión que hemos creado conjuntamente entre personal de ISDEFE y personal de la administración para la que trabajamos. La cuarta herramienta son los sistemas de procesado de información obtenida en fuentes abiertas. Y la quinta y última herramienta la constituyen los instrumentos a través de los cuales difundimos toda la información relevante de la Red (líneas de acción, resultados, etc., a través de páginas web, vídeos, folletos, etc.), porque uno de los objetivos y una de las características principales de la Red es que es una red abierta: todo lo que se investiga, todo lo que se averigua y todo lo que se consigue se pone a disposición global.

En relación con la innovación y con la red que hemos creado hemos aprendido seis lecciones que, a pesar de ser simples, consideramos que son muy útiles. La primera es 'Innovar no es una opción sino una obligación'. Como bien dice el refrán, renovarse o morir. La segunda es 'Innovan las personas', a pesar de que habitualmente se hable de empresas innovadoras. Y para ello, las personas necesitan un entorno que las motive y que las ayude. La tercera es 'Todo el mundo en una compañía tiene que innovar'. Se debe crear un caldo de cultivo para que se den las condiciones que favorezcan la innovación, porque la innovación es cosa de todos y no se puede dividir la plantilla entre los que innovan y los que están en los proyectos habituales (en ISDEFE no existe el puesto del ingeniero innovador y del ingeniero del día a día: innovar es una función inherente a todos ellos y a todo el personal que trabaja en la compañía). La cuarta lección es 'La innovación es un proceso continuo'. Se innova siempre y la innovación es consustancial al trabajo que desarrolla la persona. La quinta es 'La innovación y la motivación son inseparables'. La innovación es un proceso personal y surge de la motivación, de la necesidad intrínseca de mejorar, de hacer algo útil y distinto y que sirva a

los demás. Y por último, 'La innovación es algo endógeno, no exógeno', esto es, las actuaciones que consiguen que las personas de una organización innoven son actuaciones hacia dentro de la organización, no hacia fuera.

Un ejemplo de actuaciones de la Red Horizontes es el proyecto que tenemos con el MADOC para la investigación en la aplicación de la inteligencia artificial al sistema de combate de una brigada. Principalmente, esta colaboración se enmarca en dos líneas. La primera es un estudio prospectivo en conceptos y en inteligencia artificial básicos previos aplicados al entorno militar y enfocado fundamentalmente al empleo de fuerzas terrestres. La segunda es un estudio prospectivo del estado del arte de la inteligencia artificial en los sistemas tipo brigada en los países de nuestro entorno. Otro ejemplo de actuaciones de la Red Horizontes es un ejercicio de reflexión interna similar al ejercicio 2035 del Ejército de Tierra (aunque mucho más humilde en su alcance) al que llamamos Reto 2030, que fue lanzado en 2018 con el objetivo de identificar los desafíos que debe abordar la Administración pública en el año 2030 en los ámbitos de actuación de ISDEFE.

En todo ejercicio que intenta bucear en el futuro hay debemos hacernos tres preguntas: qué será nuevo en esa época que todavía no existe, qué existe ahora y desaparecerá y qué es lo que hay ahora y sobrevivirá en el futuro, siendo esta última la más importante. En este terreno debemos fijarnos en las películas de ciencia ficción y buscar qué artilugios aparecen, en qué año, cuáles de esos artilugios no existen y cuáles sí. Pero un ejercicio de prospectiva no puede ser solo tecnológico. El Reto 2030 es el primer estudio desarrollado que involucró a todos los actores del sistema de innovación de ISDEFE, a la Real Academia de Ingeniería, a nuestros empleados y a los organismos para los que trabajamos utilizando todos los elementos de la Red. Para realizar este ejercicio elaboramos un primer análisis a través de un proceso de reflexión interna, contrastamos los resultados con la Academia a través de los observatorios (utilizamos los grupos de reflexión con nuestros clientes y la administración para la que trabajamos para contrastar los resultados), los realimentamos y complementamos con la información procedente de fuentes abiertas y finalmente hicimos una difusión de los resultados de forma dinámica. En la primera fase del ejercicio participaron ciento veinte empleados (aproximadamente el 10% de los empleados de la compañía), las

universidades de los observatorios con los que tenemos las cátedras, académicos a título individual y los principales organismos para los que trabajamos.

En este ejercicio Reto 2030 no solo se analizaron los retos futuros a los que se enfrentará la administración para la que trabajamos sino que también se analizaron aquellos retos a los que se enfrentará nuestra organización en el futuro. En nuestro caso, como compañía a la que le impactan las famosas TIC, la transformación digital, las tecnologías rupturistas y otras del estilo, que no produce bienes sino conocimiento, cuyo principal activo son las personas y a la que le preocupa la materia prima futura, se aprovechó el ejercicio para intentar averiguar cómo será ese ingeniero del futuro y en qué tipo de organización trabajará. Y como siempre, surgen más dudas que preguntas: cómo será el ingeniero del futuro, qué formación y habilidades tendrá que tener, hacia dónde evoluciona el famoso STEM[1], cómo será la formación, qué aprenderá en la escuela, cómo serán las escuelas, cómo será su formación a lo largo de su trayectoria profesional, cuáles serán los elementos que motiven a ese ingeniero, cómo definirá su carrera profesional, cómo se articulará la relación laboral, cómo serán los equipos de futuro en los que trabajará, etc. Una de las características de nuestra empresa es el funcionamiento y trabajo en grupo. Por tal motivo nos surgieron dudas sobre cómo serán esos grupos y esos equipos en el futuro. ¿Serán cada vez más multidisciplinares, más internacionales y más integrados en red con otros equipos? ¿Habrá una mayor dispersión geográfica con trabajo remoto? ¿Qué tecnología usarán para su trabajo futuro? ¿Qué puestos de trabajo y qué perfiles de los que en estos momentos existen en nuestra compañía desaparecerán con la tecnología? ¿Cómo afectará a la organización? ¿Será una organización más plana o menor, con mayor o menor necesidad de supervisión y control? ¿Qué conocimientos se deben proteger en este caso? ¿Qué pasará con los activos físicos?, etc. Surgen muchas más dudas que certezas pero así es el impacto que tienen las tecnologías y el impacto que tiene ese ejercicio en nuestra propia organización.

1. Ciencia, tecnología, ingeniería y matemáticas (*Science, Technology, Engineering and Mathematics).*

Finalmente, Ejército, empresa y conocimiento es para ISDEFE el círculo virtuoso, ya que para poner la tecnología a disposición del Ejército hace falta generar un conocimiento en universidades, centros tecnológicos y centros de investigación que es utilizado por las empresas para construir y fabricar los sistemas que se necesitan para afrontar los retos 2035.

Nuevos retos de la seguridad internacional

Josep Piqué i Camps
Experto en Geopolítica y Geoeconomía

Nuestra seguridad y defensa descansa cada vez más y de manera sustancial en la innovación tecnológica y en la capacidad de hacer frente a los retos tecnológicos que la nueva revolución industrial, la llamada digitalización, nos ofrece en estos primeros años del siglo xxi. Cuando se habla de los nuevos retos de la seguridad internacional se está hablando de retos particularmente novedosos que implican cambios cualitativos y que incluso pueden afectar al propio concepto de guerra al que hemos estado habituados durante tantísimo tiempo a lo largo de la historia de la humanidad.

Para hablar de los nuevos retos de la seguridad internacional vale la pena hablar un poco de historia. Para entender la política internacional son fundamentales dos cosas: primero, saber que la geografía siempre está presente y que hay que mirar mucho los mapas para entender lo que pasa; y segundo, saber que de alguna forma la historia siempre vuelve, no tal como decía Marx con esa frase tan famosa «La historia se repite primero como tragedia y luego como farsa» (él hablaba de Napoleón I y Napoleón III) sino más bien en el sentido de la respuesta que dio Marc Twain cuando le preguntaron si creía que la historia se repetía: «Pues probablemente repetirse no, pero desde luego siempre rima». Lo que quiere decir que tenemos que sacar lecciones de la historia para intentar interpretar el presente y, como no, el futuro.

Por tanto, haciendo un poco de historia y hablando de la seguridad internacional más reciente, la conocida como Guerra Fría (último escenario geopolítico de la segunda mitad del siglo pasado) tuvo como resultado la ruptura de las relaciones entre países que fueron aliados durante la Segunda Guerra Mundial para derrotar a los fascismos, al nacismo y también al imperialismo militarista japonés. La Unión Soviética, los Estados Unidos y

los países de Europa Occidental, junto con otros, fueron aliados en esa guerra pero antes de que terminara empezó a quedar muy claro que sus intereses iban a ser profundamente contradictorios en el futuro inmediato, lo que ya se pudo ver en las conferencias de paz para preparar los escenarios posbélicos (Yalta sería el ejemplo paradigmático). A partir de ahí se abrió lo que hemos dado en llamar el mundo bipolar, un mundo con dos grandes polos (un bloque occidental encabezado por los Estados Unidos y otro, el bloque soviético, encabezado por la Unión Soviética) que establecieron alianzas internas. En el caso del bloque occidental, la Alianza Atlántica, que sigue estando ahí y que ha tenido que reformularse y repensarse, y en el caso del bloque soviético, la alianza militar conocida como el Pacto de Varsovia, que desapareció prácticamente con la caída del muro de Berlín y el posterior desmoronamiento de la Unión Soviética.

Pero más allá de esas alianzas también se fueron articulando diferentes tratados bilaterales, a veces al margen pero en paralelo, que de alguna manera mantenían la misma lógica. Nuestro país es un magnífico ejemplo. No formó parte de la Alianza Atlántica en sus orígenes, costó muchos años integrarse y después de diferentes vicisitudes políticas los españoles tuvimos que pasar por un referéndum en 1985 convocado por el gobierno de Felipe González para ratificar una entrada en la OTAN que había sido decidida por el gobierno de Calvo Sotelo. Por tanto, España estuvo al margen de la Alianza desde su creación a finales de los años cuarenta hasta bien entrados los años ochenta. Pero realmente no del todo, porque existía un tratado bilateral de defensa con los Estados Unidos que permitía a este país la utilización de bases militares dentro de nuestro territorio (en Zaragoza, Torrejón, Rota y Morón), situación que después fue evolucionando para pasar a ser bases de soberanía española de utilización conjunta y posteriormente a ser dos bases plenamente integradas en la estructura militar y política de la OTAN, tal y como son en la actualidad las bases de Rota y Morón.

El escenario de la Guerra fría surge de la confrontación entre dos modelos a todos los niveles. A nivel político existe una contraposición entre sistemas democráticos y sistemas basados en partido único (lo que se denominaban las dictaduras del proletariado). A nivel económico, entre economía de mercado por una parte y economías planificadas centralmente por otra. A nivel

social, en un caso hablamos de sociedades abiertas tal y como las definía Popper, fundamentadas en la libertad y en la igualdad de los individuos, y en otro hablamos de sociedades controladas por el poder político al servicio del objetivo político de llegar al socialismo. Y a nivel global, dos modelos con visiones del orden internacional absolutamente contrapuestas.

Los países pertenecientes a cada modelo tenían que pensar en cómo hacer frente a esta situación de la manera más eficaz posible. Evidentemente, la confrontación llevada a sus últimas consecuencias no era la solución. Habida cuenta de la existencia del arma nuclear estábamos ante lo que los analistas y los politólogos llamaban la Hipótesis de la destrucción mutua asegurada y por lo tanto en el escenario del equilibrio del terror. Cualquiera que fuera la potencia que iniciara la confrontación militar en sus últimas consecuencias o cualquiera que fuera la potencia agresora, el resultado iba a ser absolutamente insufrible para ambas partes y en cualquier caso con un coste absolutamente inasumible, que podía llegar incluso a la destrucción del planeta. Por tanto, era un escenario diferente al de guerras anteriores en las que al final una potencia se imponía sobre la otra en los campos de batalla.

Esto dio lugar a lo que se ha conocido como la Trampa de Tucídides, concepto que ya forma parte de la terminología habitual cuando se habla de las amenazas a nuestra seguridad. Tucídides, el gran historiador clásico griego, escribió sobre las guerras del Peloponeso y en particular sobre la confrontación entre una potencia naval (Atenas) y una potencia terrestre (Esparta). La tesis de Tucídides dice que cuando hay una potencia establecida y otra cuestiona su hegemonía, más tarde o más temprano se cae en la trampa y la confrontación es inevitable. Eso fue así en el caso de Atenas y Esparta, sin ninguna duda. Esta tesis incluso se ha analizado desde el punto de vista académico. Hay un libro titulado Destinados a la guerra que recoge unas experiencias realizadas en Harvard para analizar si en dieciséis casos distintos acontecidos en los últimos dos mil años se cumple o no la famosa Trampa de Tucídides. En todos ellos la trampa se impuso de manera absolutamente implacable y se llegó a la confrontación militar directa, excepto en tres casos.

Uno fue la disputa entre España y Portugal por los nuevos dominios coloniales que se abrieron a partir de la era de los descubrimientos. En esta ocasión la situación no desembocó en una guerra sino que gracias a una intermediación papal se llegó a un

acuerdo (el Tratado de Tordesillas) que de alguna manera partía el mundo conocido entre las dos potencias.

Otro caso de no cumplimiento de la Trampa de Tucídides fue el que se derivó de la aceptación por parte del Reino Unido de que había una nueva potencia que iba a ser dominante, hegemónica y con la que no convenía enfrentarse sino acomodarse: los Estados Unidos. Cuando empieza la irrupción de los Estados Unidos como gran potencia, el Reino Unido incluso renuncia a uno de sus principios fundamentales en términos de seguridad. Todos los grandes imperios en el pasado han dominado las rutas marítimas. Así fue en el caso de España, Portugal, Países Bajos y Reino Unido y lo está siendo en el caso de los Estados Unidos y en cierta medida también en el de China. Pero el Reino Unido tenía un principio fundamental: su flota (la Royal Navy) tenía que ser por lo menos igual a la suma de las flotas de las dos potencias competidoras que seguían a continuación. Ese principio no lo aplicó con los Estados Unidos, aunque sí con los países europeos. De hecho, una de las explicaciones de la Primera Guerra Mundial fue precisamente la pretensión del Káiser alemán de disponer de una armada que fuera equiparable a la del Reino Unido, lo que para este país fue literalmente *casus belli*.

Y el tercero fue precisamente la Guerra Fría, por el miedo a la destrucción mutua asegurada y por el equilibrio del terror basado en la amenaza nuclear. Los teóricos de la geopolítica sitúan el inicio de la estrategia del bloque occidental para hacer frente a ese equilibrio en el Telegrama Largo de George Kennan (quien en aquellos momentos estaba trabajando en la embajada de Moscú), punto de partida de la estrategia de contención adoptada por Occidente con respecto a la amenaza soviética. La pieza fundamental de esta doctrina fue la paciencia estratégica basada en la confianza de los valores de occidentales: aguantar, ser conscientes de las fortalezas propias y saber que enfrente había alguien que no necesariamente seguía la lógica de la razón pero sí que era muy sensible a la lógica de la fuerza, y que por lo tanto requería de respuestas específicas puntuales en cada momento.

En ese escenario vivimos prácticamente desde la segunda mitad del siglo XX. Un escenario que era cambiante. Los que vivimos esa época pensábamos que iba a ser muy sostenible en el tiempo, que lo íbamos a vivir a lo largo de nuestro horizonte vital y que iba a continuar en el horizonte de nuestros hijos y de nuestros

nietos. Nos parecía que estábamos ante una especie de empate permanente, con sus vicisitudes, sus conflictos puntuales y con su lógica evolución interna. Por lo que respecta a la Unión Soviética, no es lo mismo la época de Stalin que la época de Krushov, ni la de Brézhnev que la de Gorbachov, sin olvidar otras épocas protagonizadas por secretarios generales del partido comunista más o menos efímeros como Chernenko o como Andrópov. El bloque soviético pasó por una etapa profundamente agresiva articulada sobre el Komintern de la internacional comunista, con una clara voluntad de usar los partidos como cabeza de playa para la extensión del modelo soviético y de su ideología.

Después de la etapa de contención pasamos a otra de coexistencia pacífica, sobre todo en la época de Brézhnev, caracterizada por la aceptación de que ninguno de los dos bandos iba a poder asegurarse su supremacía, por lo que se debían limitar los riesgos para poder coexistir y convivir. Esto facilitó llegar a acuerdos que en época de Stalin hubieran sido impensables, como los de limitación de armas estratégicas y tácticas (que por cierto ahora están siendo cuestionados y algunos denunciados).

Pero en este contexto también se han vivido situaciones delicadas. Probablemente, la más peligrosa se vivió a principios de los años sesenta con la que fue conocida como crisis de los misiles en Cuba. Y lo fue porque para los Estados Unidos la instalación de misiles en la isla de Cuba, eventualmente con cabezas nucleares y a pocas millas de sus costas, constituía una amenaza vital absolutamente insoportable. Por eso el presidente Kennedy mantuvo frente a Krushov la amenaza absolutamente taxativa y creíble de ir a la guerra si no se retiraban.

También hubo muchos cambios de bando a raíz de las numerosas guerras sustitutivas de una confrontación global que se produjeron en el sudeste asiático, en el continente africano, en américa latina o en cualquier lugar del globo. El más relevante desde el punto de vista occidental se produjo a raíz de la derrota norteamericana y la retirada de los Estados Unidos de Vietnam, que hizo caer a países como Laos o Camboya en lo que parecía que iba a ser la decantación de todo el sudeste asiático hacia el bloque soviético. Cosa que finalmente no ocurrió merced al golpe de estado de Suharto en Indonesia (otro episodio muy notable), que impidió que esa región cayera en manos comunistas y permitió que Occidente pudiera mantener sus intereses vitales en buena parte de ella.

Pero además de este ha habido muchos otros episodios. Es verdad que había un cierto respeto a los derechos adquiridos, particularmente en la conferencia de Yalta. Cuando las tropas del Pacto de Varsovia invadieron primero Hungría en el año 1956 y luego Checoslovaquia en el año 1968, la reacción de Occidente fue básicamente mirar hacia otro lado al entender que estos hechos sucedían en lo que se podía considerar como área de influencia de la Unión Soviética y que por lo tanto no cabía utilizarlos como elementos de confrontación. En paralelo, en muchos otros lugares del mundo pero particularmente en América Latina las respuestas a las amenazas desarrolladas habitualmente a través de tácticas guerrilleras fueron golpes militares apoyados por los Estados Unidos (como en Chile y Argentina, entre otros). Para el bloque soviético esta región era de alguna manera área de influencia del país norteamericano, por lo que las respuestas no podían ser puestas en cuestión. Más avanzado en el tiempo, en los años 1973/74 tuvo lugar la Revolución de los Claveles en Portugal, a la que siguió un período de gobiernos provisionales en los que hubo cierto riesgo de que ese país se decantara por la esfera soviética. Finalmente eso no fue así, ya que hubo una reacción occidental muy clara de apoyo a los elementos democráticos derivados de la revolución y Portugal siguió siendo un miembro activo de la Alianza Atlántica y un claro socio de Occidente.

Pero más allá del respeto por las áreas de influencia anteriormente mencionadas hubo también episodios muy notables. Probablemente, el ejemplo más paradigmático sea Egipto. Por una serie de razones, entre otras el conflicto con Israel y la torpeza franco/británica respecto a su política, Egipto pasó a ser un aliado muy estrecho de la Unión Soviética. Y así fue hasta la guerra de Yom Kipur. Tras ella, en el año 1973 y después de los acuerdos de paz de Camp David, Egipto decidió literalmente cambiar de bando y pasar a ser un aliado estratégico de los Estados Unidos. Eso, unido a la firma de la paz con Israel, le acabó costando la vida al presidente egipcio que puso en marcha el proceso (Anwar el-Sadat). Hoy Egipto sigue siendo hoy uno de los principales aliados de los Estados Unidos y el segundo receptor de ayuda militar norteamericana en todo el mundo tras Israel.

Otro episodio notable que anticipaba lo que ya ha acontecido fue la Revolución de Irán, un acontecimiento traumático en el escenario internacional y en la división entre bloques. A pesar

de que esta fue una revolución fundamentalmente antinorteamericana, no se podía identificar con el avance soviético en la región sino que tenía su propia lógica interna, como después se ha demostrado. Pero fue una revolución política y un cambio geopolítico que no se podría interpretar y explicar sin partir de la lógica de la división entre bloques.

En este punto conviene recordar que los cambios de alianzas (enemigos que pasan a ser amigos y amigos que pasan a ser enemigos) se han producido a lo largo de la historia de la humanidad, pero estos ejemplos recientes pueden servir de aliciente intelectual porque quizás muchas vicisitudes pueden llegar a ser aplicables a numerosos conflictos que vemos hoy en día.

Más allá de los cambios de bando conviene hacer un repaso a lo que fue la evolución del equilibrio nuclear geoestratégico, que también ha pasado por fases sucesivas. En un primer momento los Estados Unidos tuvieron el monopolio nuclear, pero al cabo de poco tiempo la Unión Soviética pasó a tener también la bomba. A ese duopolio se le añadió China y después hubo una cierta proliferación: India, Pakistán, Francia, el Reino Unido e Israel (aunque públicamente no lo haya reconocido nunca). Esta situación fue generando amenazas estratégicas y tácticas. Ya se ha comentado la crisis de Cuba, en la que el despliegue de misiles rusos significaba una amenaza directa y vital para los Estados Unidos a pocas millas de su territorio desde una isla controlada a todos los efectos por la Unión Soviética. En esta crisis jugó un papel esencial el valor estratégico de los bombarderos por la parte norteamericana y de los submarinos por la parte soviética.

Pero hay otros episodios que fueron clave en los que la geografía tuvo de nuevo mucho que ver. No hay que olvidar que los Estados Unidos están en un continente alejado, entre dos grandes océanos y, salvo el caso de Cuba, sin amenazas geográficas directas. No así la Unión Soviética, que está en Eurasia y tiene muy cerca de su ámbito de influencia una Europa Occidental alineada con los Estados Unidos. En este ámbito fue clave el momento en que la Unión Soviética decidió ir más allá de los misiles estratégicos de carácter intercontinental y decidió desplegar misiles de corto y medio alcance (los llamados SS20) en territorios de Europa de influencia soviética para amenazar directamente a los aliados europeos de los Estados Unidos. La respuesta de la Europa Occidental, que se produjo gracias sobre todo a la determinación

de algunos líderes como el canciller Helmut Schmidt en Alemania y François Mitterrand en Francia y que generó un enorme debate social, fue permitir a la Alianza Atlántica la instalación de misiles de corto y medio alcance en territorio europeo (los Pershing y los Cruise). A partir de ese momento la Unión Soviética pasó a tener una amenaza estrictamente continental de medio y corto radio además de la amenaza intercontinental. Es cierto que Europa Occidental estaba amenazada por misiles de corto y medio alcance, pero en este escenario los Estados Unidos tenían únicamente la amenaza estratégica intercontinental. Este proceso finalizó con un paso adelante de la potencia norteamericana que probablemente tuvo mucho que ver con el final de la Guerra Fría: el desarrollo de escudos antimisiles para neutralizar esa amenaza y quedar así salvaguardados de algún tipo de agresión. Este paso adelante coincidió fundamentalmente con la época del presidente Ronald Reagan. Por entonces la Unión Soviética estaba ya en proceso de descomposición por razones políticas, internas y de cohesión territorial. El resultado final fue, entre otras muchas cosas, la gran victoria Occidental en la Guerra Fría sin paliativos.

Efectivamente, la rendición del bloque soviético fue incondicional. Esto llevó a muchos a pensar que se abría una nueva fase que podría ser mucho menos peligrosa que la anterior, dominada por una única superpotencia (los Estados Unidos) que iba a propiciar la generalización de los valores occidentales al resto del planeta. Dicho de otra manera, iba a llegar el fin de la historia (como decía Francis Fukuyama), porque si la democracia representativa se iba generalizando y abrazaba a los antiguos países satélites de la Unión Soviética (cosa que sucedió), a la propia Rusia (cosa que en un momento determinado pareció que iba a suceder) y hasta incluso a países emergentes en aquel entonces (como China); si se iba a acabar aceptando la democracia y la libertad a medida que el crecimiento económico permitía el desarrollo de clases medias; y si asistíamos a una generalización de sistemas democráticos, las confrontaciones podrían ser resueltas por vías pacíficas. Lo mismo cabría decir en términos económicos. La victoria de Occidente llevó a pensar que, frente al fracaso de las economías planificadas, la economía de mercado era el único sistema posible que garantizaba la provisión de bienes públicos y privados y la satisfacción de las necesidades ciudadanas, y que por lo tanto la economía de mercado sobre la base de la iniciativa privada

también iba a generalizarse. Obviamente, eso también implicaba que íbamos a vivir en sociedades abiertas y libres y que podría haber un orden liberal internacional encabezado por los Estados Unidos que iba a evitar el uso ilegítimo de la fuerza para resolver conflictos. La primera guerra del Golfo podría ser un ejemplo paradigmático de que íbamos a asistir a un respeto al derecho internacional y a los derechos humanos, y que esa colaboración global iba a tener una base fundamental en el multilateralismo y en el libre comercio, que se iba a extender por doquier. Y si había libre comercio, libre circulación de factores productivos y respeto a las normas asistiríamos al fin de la historia tal y como la habíamos conocido con anterioridad, caracterizada por el desarrollo de permanentes conflictos, normalmente además de carácter bélico.

Pero pronto vimos que esa especie de Arcadia feliz que parecía que iba a caracterizar la primera mitad de este siglo XXI iba a tener muy poco que ver con la realidad. Lo descubrimos de una forma abrupta el 11 de septiembre de 2001, cuando la entonces única superpotencia sufrió un ataque directo y además con un componente simbólico muy importante. Cuando cayeron las Torres Gemelas de Nueva York lo que se derrumbó fue probablemente el símbolo más claro y orgulloso del capitalismo. Fue un ataque en toda regla al sistema económico norteamericano. Pero además se vio como un avión comercial se estrellaba nada menos que contra el Pentágono, sede del poder militar teóricamente omnipotente de la hasta entonces única superpotencia. Estamos hablando de una amenaza asimétrica importantísima para nuestra seguridad: el terrorismo internacional, normalmente de matriz yihadista.

Paradójicamente, la victoria sin paliativos de Occidente implicó el proceso de desoccidentalización del planeta más rápido y más vertiginoso que jamás hubiéramos podido imaginar. En contra de lo que podía parecer intuitivo sucedió algo contraintuitivo: en lugar de generalizarse los valores occidentales surgieron muy rápidamente otros poderes y otras potencias que no aceptaron ese pretendido nuevo orden basado en la hegemonía norteamericana y en los valores de Occidente, y que pasaron a reivindicar su papel. El ejemplo más claro es, obviamente, China.

China está volviendo a su ser. Más que un país es una civilización y una cultura que descansa sobre las aportaciones de Confucio. Durante sus tres mil doscientos años de existencia y hasta

mediados del siglo XIX China siempre fue el país y la economía más importante del mundo. China significa 'Imperio del centro' y siempre había considerado a todos los que están a su alrededor como objeto de vasallaje o directamente como bárbaros. Eso incluía, por ejemplo, al Imperio Británico. Hay una anécdota muy conocida de cuando el Rey Jorge II envió un emisario a la corte del emperador chino para pedir el establecimiento de relaciones diplomáticas y la apertura del comercio. El emperador, con enorme displicencia, le dijo que cómo él, un rey bárbaro, había tenido la osadía de pedir condiciones en relación de igualdad nada menos que con el imperio chino.

Pero a partir de mediados del siglo XIX empezó lo que los propios chinos llaman el siglo de la humillación: cien años en los que las potencias occidentales, primero europeas y luego los Estados Unidos, pasaron por encima de la hegemonía china y la sometieron a humillaciones, incluidas invasiones muy importantes. Lo chinos interpretan esos cien años como resultado de su inferioridad con respecto a la capacidad tecnológica de las potencias occidentales derivada de las revoluciones industriales (tanto de la máquina de vapor como de la electricidad o del motor de combustión). Han aprendido esa lección, no quieren que vuelva a suceder y saben que la pugna fundamental, que tiene sus derivadas militares, es básicamente tecnológica. El siglo de la humillación para los chinos acaba en 1949, finalizada ya la Segunda Guerra Mundial, después de la guerra civil en China y constituida la República Popular. En las resoluciones del último congreso del Partido Comunista (el decimonoveno) consta explícitamente el objetivo de China: cien años después China tiene la ambición, la voluntad y la estrategia para ser la gran potencia global dominante en la Tierra a mediados del presente siglo (en concreto, en 2049). Y está claramente en eso, lo que conviene tener muy presente para entender los nuevos desafíos. Hay una anécdota muy ilustrativa relacionada con este deseo de China de volver a su ser. En una ocasión le preguntaron a Niall Ferguson, historiador británico escocés muy brillante y muy heterodoxo, si creía que el siglo XXI iba a ser el siglo de China y su respuesta fue: «¿Por qué no, si todos lo han sido menos el siglo XX?». Era una manera de decir que habrá que ir aceptando esa realidad y esa estrategia, que tiene aspectos multidireccionales que para algunos responde a un planteamiento de cien años. Existe un libro escrito

titulado El maratón de los cien años, escrito por un antiguo oficial de inteligencia norteamericano, en el que se dice que dentro de la estructura china de poder siempre ha habido una parte claramente orientada a desarrollar una estrategia que en cien años le permitiera recuperar su papel tradicional e histórico y suplantar a los Estados Unidos como principal superpotencia. Hay muchas manifestaciones de esa estrategia multidireccional. La capacidad comercial es del todo punto evidente y por eso estamos hablando de las guerras arancelarias y de las guerras comerciales. La evolución de China ha sido absolutamente espectacular, con unas tasas de crecimiento en su economía sin precedentes, pero también en cuanto a presencia empresarial en el mundo. La presencia de China en África, en América latina o cada vez más en Europa es absolutamente indiscutible. Pero además se está implementando con varias iniciativas estratégicas muy relevantes, siendo la más conocida la famosa Ruta de la Seda. Las nuevas rutas comerciales se basan en la Ruta de la Seda tradicional, la que comerciaba con seda y especias entre China y Europa descrita por Marco Polo, que ahora se recupera por la vía tradicional terrestre para llegar a Europa a través de Asia central, el Caspio, el Cáucaso y el Mar Negro. Esta ruta lleva aparejadas enormes infraestructuras de transporte que ligan estratégicamente a todos los países de paso a la propia estrategia de China. Hace relativamente poco, para gran enfado europeo y de los Estados Unidos, el anterior gobierno italiano firmo un acuerdo estratégico con China precisamente para facilitar que la nueva Ruta de la Seda pudiera utilizar la península italiana para su desarrollo. Pero más allá de esa ruta tradicional terrestre, China ha entendido que si quiere ser una potencia global tiene que ser también una potencia aeronaval y compaginar esto con sus intereses políticos, comerciales, económicos y empresariales. Por ello ha desarrollado una nueva Ruta de la Seda Marítima de doble sentido (entrada y salida) y de doble uso (combina puertos comerciales con bases navales militares), coloquialmente conocida como el collar de perlas chino.

El punto de partida para el establecimiento de esta ruta obedece a la obsesión por el Estrecho de Malaca. Este estrecho es la conexión entre el Pacífico y el Índico y por lo tanto la entrada y salida natural de los *inputs* y *outputs* que China necesita para seguir financiando su enorme proceso de crecimiento y al mismo tiempo su presencia global. Pero el estrecho, que por definición es muy angosto y por lo tanto fácilmente bloqueable, está rodeado de fuerzas navales y aeronavales estadounidenses, muy presentes en torno a él y en el Mar de China Meridional. Personalmente defiendo que va a ser el centro de gravedad del mundo en este siglo, porque va a ser un escenario de tensiones cada vez más importante. Para obviar el riesgo de bloqueo del Estrecho de Malaca China podría intentar controlarlo, lo que pasaría necesariamente por desplazar a los Estados Unidos del Mar Meridional, o bien podría obviarlo geográficamente a través de un corredor ya establecido con países aliados desde territorio chino que permita llegar al Índico sin necesidad de atravesar el Estrecho.

El origen del collar de perlas se sitúa en Bangladesh, en un puerto muy importante que está al oeste de la capital (Daca), parte del cual está controlado por China. Pasa por Sri Lanka (la antigua Ceilán portuguesa), donde China controla el principal puerto, lo que le permite obviar al subcontinente indio (India y China han sido enemigos históricos; de hecho, si no hubiera existido el Himalaya las confrontaciones hubieran sido más intensas de lo que lo han sido históricamente). La ruta bordea el sur de la India y vuelve a subir por el Índico Occidental hasta Pakistán

(tradicional aliado de China y también de la India). En este país China tiene a su disposición el enorme puerto de Gwadar, de doble uso, situado al oeste de Karachi. Desde Pakistán la ruta sigue hasta el continente africano saltándose la península arábiga por razones obvias. Desde la costa africana oriental lo natural es conectar con el Mediterráneo para después llegar al Atlántico. Para ello hay que desplazarse hacia el Mar Rojo a través del Golfo de Adén atravesando el estrecho de Bab el Mandeb (que es casi tan importante como el de Ormuz) y después atravesar el Canal de Suez para entrar en el Mediterráneo. En el estrecho de Bab el Mandeb hay unos países complicados. Al norte está Yemen, un país que está inmerso en guerras civiles, en una de las cuales uno de los bandos está apoyado por Irán y otro bando está apoyado fundamentalmente por Arabia Saudí y de manera diferente por los Emiratos Árabes Unidos. Por lo tanto, ni es estable ni es fiable. Al sur están Somalia y Eritrea, dos estados semifallidos que no controlan su territorio ni sus mares; de hecho han tenido que recurrir a fuerzas navales y aeronavales básicamente occidentales para combatir la piratería (Operación Atalanta). Pero además de estos dos países fallidos está Yibuti, un pequeño país relativamente desconocido hasta hace poco. Yibuti fue una colonia francesa hasta bien entrados los años setenta (de hecho todavía hay presencia militar francesa y de otros países). Su importancia es tal que los Estados Unidos decidieron que su única base militar permanente en el continente africano iba a estar en ese país. Pero se da la casualidad nada casual de que China ha establecido en ese territorio una base militar incluso más importante que la norteamericana, lo que le permite asegurar el libre paso por Bab el Mandeb, acceder al Mar rojo y llegar a Suez para concluir en el Mediterráneo. Una vez en este mar, el puerto europeo más próximo es el de Atenas (El Pireo), que precisamente está controlado por China. A partir de ahí la ruta avanza hacia el Mediterráneo Occidental hasta llegar a Italia (que ya se ha comentado) y a la península Ibérica, en la que hay diferencias: en el caso de Portugal, la presencia china pasa fundamentalmente por el control de su sistema energético, tanto de la principal distribuidora (EDP, Energías de Portugal) como de la red eléctrica equivalente a la nuestra (Red Eléctrica Portuguesa, con mayoría de capital chino); en el caso de España, lo que hay es una presencia creciente en los puertos del Mediterráneo, de momento estrictamente comercial.

Todo esto constituye un buen ejemplo de lo que está desarrollando China, que además entiende que la gran pugna se tiene que desarrollar en los ámbitos terrestre, aeronaval, empresarial, estratégico y de las alianzas. Pero sobre todo, China entiende que la gran confrontación se desarrolla en el espacio y el ciberespacio y que la gran pugna es la tecnológica (recogiendo la enseñanza del siglo de la humillación, es decir, nunca más su preponderancia va a ser cuestionada por una inferioridad tecnológica). Hace ya mucho tiempo que China ha dejado de ser la fábrica del mundo (ahora lo son la India, el sudeste asiático o incluso países africanos como Etiopía, que producen manufacturas con costes salariales muy bajos). Hoy es una gran potencia tecnológica, y en algunos casos la gran potencia tecnológica. Ha hecho un esfuerzo descomunal en sus universidades y en sus centros de investigación y ha aprovechado la entrada de empresas occidentales en su territorio para condicionarlas con prácticas que son completamente contrarias a la OMC (las empresas europeas y norteamericanas que quieren estar presentes en el mercado chino normalmente deben hacerlo a través de empresas chinas controladas por el estado, y la condición fundamental para poder hacerlo es que tienen que ceder la tecnología). Dejando aparte la piratería (que también), China tiene una absorción de tecnología absolutamente espectacular que va ligada al esfuerzo que está haciendo a nivel universitario: no solo los egresados de las universidades chinas en las áreas de STEM triplican o cuadriplican los egresados en las universidades norteamericanas sino que además centenares de miles de estudiantes chinos que estudian en universidades occidentales regresan a su país una vez aprendida la tecnología (algunos pensaban ingenuamente que esos estudiantes chinos se iban a quedar en los países en los que realizaron sus estudios universitarios una vez descubrieran la libertad). Para muchos observadores esto está haciendo que China tome la delantera en campos tan sustanciales como la inteligencia artificial, con todo lo que eso comporta. Porque cuando se habla de inteligencia artificial se está hablando del desarrollo de las infraestructuras necesarias para permitir una capacidad de respuesta inmediata: el 5G. Al hablar del conflicto de intereses entre Huawei y los Estados Unidos, algunos medios de comunicación occidentales se refieren a ello como otro episodio de la guerra comercial entre los Estados Unidos y China, pero en realidad no es así. Lo sustancial en esta contienda es la pugna

tecnológica y el interés en dominar las infraestructuras de redes que van a permitir el internet de las cosas (IoT)[1], a lo que van asociados fenómenos tan importantes como el *blockchain* o la utilización de la nube (el *cloud*), por poner ejemplos absolutamente tópicos. A este respecto, el presidente ruso Putin pronunció una frase que es muy gráfica: «Quien domine la inteligencia artificial dominará el mundo». La nueva confrontación estratégica, esta nueva guerra fría, esta nueva Trampa de Tucídides en la que corremos el riesgo de volver a caer, pasa fundamentalmente por la pugna tecnológica. De ahí que esta situación sea angustiosa para los Estados Unidos.

Incluso se podría ir un poco más lejos. Si pensamos en la guerra, desde tiempos inmemoriales ha consistido en ver quien era más eficaz a la hora de lanzarse cosas: piedras en la Edad de Piedra, flechas, lanzas, tiros y ahora nos amenazamos con tirarnos misiles. Probablemente el núcleo de la preocupación estratégica de la Alianza Atlántica, del Pentágono y de otras muchas instancias (también del Estado Mayor español) es saber qué se puede hacer para que eventuales adversarios no neutralicen nuestros sistemas de información, hackeándolos o simplemente neutralizándolos, de tal manera que si llegase un momento en que hubiese que dar una respuesta no nos encontrásemos con que no somos capaces de utilizarlos. La mera existencia de esta posibilidad hace que la diferencia sustancial que todavía existe en capacidad nuclear entre los Estados Unidos y China pase a ser menos relevante, cuando no secundaria. No hace ni dos años que China destruyó uno de sus satélites desde su territorio, algo que pasó relativamente desapercibido. Según la versión oficial china, se trataba de un satélite meteorológico, aunque probablemente era algo más. Pero lo realmente relevante fue que China demostró que podía destruir un sistema satelital, con todo lo que eso implica desde el punto de vista de nuestra seguridad y de nuestra defensa colectiva.

China está demostrando que internet y la revolución digital se pueden convertir claramente en un instrumento de control y de dominación social, en contra de lo que pensábamos los occidentales en cuanto a que creíamos que iban a ser unos instrumentos de libertad que permitirían a los individuos ampliar su capacidad

1. *Internet of Things*.

para acceder a la información relevante y para tomar decisiones desde el libre albedrío como nunca con anterioridad. Esto comporta un debate ético de fondo sobre los datos, nueva materia prima y factor de producción que ha sustituido a los tradicionales tierra, trabajo y capital. Si le preguntásemos a un estadounidense de quién son los datos, probablemente contestaría que cree que son suyos. En la práctica, los datos son de las grandes empresas tecnológicas (de las GAFA), que los utilizan para desarrollar sus propios sistemas de negocio de una manera absolutamente abrumadora y que descansan su modelo de negocio en una materia prima o en un factor de producción que teóricamente no es suyo, estando así aceptado socialmente en los Estados Unidos hasta ahora (otra cosa es el debate de si el poder monopolístico de esas empresas obliga a algún tipo de legislación *antitrust* como en su día se hizo con las *babybells* para romper el monopolio de las telecomunicaciones en los Estados Unidos). Si le preguntásemos de quien son los datos a un europeo, no habría debate: los datos pertenecen a cada individuo porque se está hablando de privacidad y de intimidad. No es casualidad que haya sido la Unión Europea la única que ha legislado sobre esto, porque va íntimamente ligado al concepto de libertad individual que deriva del humanismo cristiano y sobretodo de los valores asociados al Siglo de las Luces y a la Ilustración con los que se conforman las sociedades liberales más modernas y abiertas. Pero si la pregunta se la hiciésemos a un oriental en general y a un chino en particular, la respuesta sería muy llamativa: los datos son del poder y por lo tanto el poder tiene todo el derecho a utilizarlos en beneficio de su proyecto político. Un razonamiento que tiene una raíz cultural propia, pues China no ha vivido la Ilustración y está basada en el pensamiento de Confucio: la armonía está por encima de la libertad. Parafraseando a Goethe: «La injusticia es preferible al desorden». Hay todavía un concepto más claro: la colectividad es más importante que el individuo. El hecho de que en el mundo estén avanzando ese tipo de conceptos que de alguna manera desplazan el centro de gravedad que la libertad y la dignidad de los individuos han tenido siempre en Occidente poniendo en su lugar determinados proyectos políticos de control social constituye uno de los principales riesgos y retos de nuestra seguridad colectiva, lo que tiene unas consecuencias espectaculares y constituye un debate muy de fondo.

Si planteásemos el nuevo escenario mundial como una película veríamos que hay dos claros actores protagonistas: China y los Estados Unidos. El país norteamericano está en fase de repliegue en todos los terrenos, incluidos el militar y el estratégico, como hemos visto recientemente en Siria (donde ha abandonado a sus tradicionales aliados kurdos). Pero no solo en Oriente Medio: cada vez más se desentiende de la seguridad y de la defensa de Europa y de países tradicionalmente aliados como Japón o Corea del Sur, a los que ha pedido que asuman más responsabilidades en su propia seguridad y en su propia defensa y que no descansen exclusivamente en la protección estadounidense. Paradójicamente, quien ha encabezado el bloque occidental y la defensa y la proyección de sus valores está ahora protagonizando la resistencia frente a lo que pueda venir de fuera. Es el retorno al unilateralismo, el abandono y la zozobra del multilateralismo, la vuelta al proteccionismo y la renuncia al libre comercio, entre otras muchas cosas. Todo esto lleva al debilitamiento del vínculo atlántico entre los Estados Unidos y Europa, que tradicionalmente ha ligado un Reino Unido que precisamente también está en repliegue, siendo el Brexit un ejemplo absolutamente paradigmático del abandono de las responsabilidades globales y de la renuncia a estar presente en grandes procesos de integración (como puede ser la Unión Europea).

Y eso nos lleva a preguntarnos sobre cuál es el papel de Europa en esta película. Obviamente Europa no puede ser protagonista porque no tiene capacidad para eso, pero se podría pensar en la categoría de actores de reparto, que muchas veces juegan un papel fundamental para entender la trama y que a veces incluso son merecedores de óscar. El principal actor de reparto es Rusia, sin ninguna duda. Pero hay otros actores que a pesar de tener menos intensidad son cada vez más relevantes, como por ejemplo Turquía, Irán o la India (que no tardará mucho en ser el gran actor de reparto).

Las posibilidades de Rusia para jugar un papel como potencia global se ven condicionadas por su posición geográfica. Rusia siempre ha tenido la obsesión estratégica de garantizar su seguridad frente a eventuales invasiones y ataques procedentes del exterior, toda vez que han sufrido muchas tanto desde oriente como desde occidente. Pero siempre ha tenido muy claro que la mejor manera de defender sus fronteras es expandiéndolas, tal y como

decía la emperatriz Catalina. Así surgió la idea de la Unión Soviética, culminación del sueño imperial que el mismísimo Pedro el Grande podría haber tenido en su cabeza: dominar el Báltico, buena parte de Europa Central y Oriental (desplazando su eje de seguridad cuanto más hacia occidente mejor, partiendo incluso a Alemania por la mitad), el Mar Negro, el Cáucaso, el Caspio, Asia Central y llegar hasta el Mar de Japón. Todo eso fue la Unión Soviética con sus países satélites, sobre cuya desaparición Putin llegó a decir que fue la principal catástrofe geopolítica del siglo XX, cosa que para un ruso probablemente sea así pero no para el resto del mundo. Una anécdota muy reveladora fue la frase pronunciada por Obama en un momento determinado: «No hay que preocuparse excesivamente por Rusia porque no puede ser otra cosa que una potencia regional». Rusia no tiene un PIB con el que poder aspirar a ser una potencia global, no tiene población suficiente (algo más de cien millones de habitantes) y además su estructura productiva es muy poco sofisticada. Pero sin embargo está haciendo un enorme esfuerzo en el ámbito tecnológico, en el espacio y ciberespacio (sobretodo), en la tecnología militar y en el uso de la energía (que es algo que le sobra). Y además tiene otros dos elementos a tener en consideración. Uno es la potencia militar (el *hard power*), que ya utilizó a principios de siglo en Georgia cuando vio amenazados sus intereses militares en el Cáucaso, que ha utilizado después en Ucrania o que ahora está utilizando de manera absolutamente clara y masiva en la guerra de Siria. Y otro elemento a considerar es que Rusia tiene un objetivo: recuperar el ámbito de influencia que tuvo en su día la Unión Soviética y reivindicar su papel como gran potencia indispensable a la hora de analizar cualquier conflicto por muy lejos de Moscú que esté; es decir, que se tenga que contar con Rusia de alguna manera para cualquier cosa que pase en el mundo y desmentir así la opinión del presidente Obama.

Un elemento adicional de interés militar es la tradicional obsesión de Rusia por acceder a las llamadas aguas calientes. Y de nuevo padece la maldición de la geografía. Para pasar desde el Báltico al Atlántico ha tenido que atravesar los hostiles estrechos escandinavos incluso hasta en la época de la Unión Soviética. Para pasar del Mar Negro al Mediterráneo tenía de pasar por otros estrechos hostiles (el Bósforo y los Dardanelos, de ahí la importancia creciente del entendimiento entre Rusia y Turquía

que se está produciendo actualmente). Con respecto al acceso directo al Índico, el imperio británico supuso un freno a su voluntad expansionista (en el siglo XIX a la pugna entre el imperio de los zares y el imperio británico para acceder a este océano se le llamaba el Gran Juego). El deshielo del Ártico está abriendo un escenario nuevo que a buen seguro dará mucho que hablar como gran desafío estratégico en este siglo, no solo porque va a abrir nuevas rutas marítimas y porque va a permitir el acceso a todo tipo de materias primas o energéticas (incluidas tierras raras) sino también por su utilización militar, por el control del polo norte y por la posibilidad que le va a dar a Rusia de acceder directamente al Atlántico sin pasar por estrechos hostiles. En cuanto al acceso al Pacífico, personalmente creo que Putin se acuerda todos los días de los ascendientes de quien decidió vender Alaska a los Estados Unidos, porque de no haberlo hecho el Estrecho de Bering estaría bajo su dominio exclusivo.

Todo esto marca un escenario de desafíos en este nuevo siglo: amenazas asimétricas que no eran específicas de la Guerra Fría, como el terrorismo internacional; la voluntad hegemónica de China, con valores muy distintos; la agresividad de Rusia y su ansiedad histórica; y un cierto retorno de los imperios persa y otomano por parte de Irán y Turquía, respectivamente.

Irán, nostálgico de lo que fue el imperio persa y siempre en conflicto con los países árabes, está consiguiendo acceder al Mediterráneo a través de su política exterior. Cabe recordar que eso fue lo que intentaron los persas cuando pretendieron invadir Europa a través de Grecia antes de ser detenidos por tierra en las Termópilas y por mar en Salamina. En la actualidad Irak no es un aliado de Irán, pero no tiene un gobierno totalmente hostil como el anterior de mayoría chiita. En Siria tiene un aliado evidente en el gobierno de Bashar al-Ásad y en Líbano tiene una presencia indiscutible a través de Hezbollah, lo que le facilita ese acceso al Mediterráneo.

Pero probablemente un ejemplo paradigmático de cambio de orientación es Turquía. El imperio otomano siempre fue un puente entre Asia y Europa, con pretensiones clarísimas hacia esta última. Los otomanos llegaron a las puertas de Viena y ocuparon los Balcanes durante mucho tiempo, de ahí que haya una mayoría musulmana en Bosnia o en Albania. También tuvieron presencia en el continente asiático, concretamente en la penín-

sula de Anatolia (nunca en Asia central debido a conflictos de intereses con China y Rusia, principalmente). Pero la Primera Guerra Mundial significó la desaparición del imperio otomano (también del ruso, del austro-húngaro y del alemán). A partir de entonces Turquía inició un proceso de occidentalización con Mustafá Kemal Atatürk. El que fuera imperio otomano, al que se le llamaba el enfermo de Europa, decidió que su futuro debía pasar por la occidentalización de todo, incluso de las costumbres y de la manera de vestir, lo que culminó con la voluntad de integrar a Turquía en la Unión Europea. Esto fue así durante el último siglo, pero hoy en día las cosas han cambiado bajo la perspectiva de Erdogan. Turquía está recuperando el espíritu otomano de puente entre Asia y Europa. De hecho está tomando decisiones muy contradictorias en relación a su permanencia en la Alianza Atlántica, incluida la compra de misiles a los rusos o los acuerdos con estos para controlar el norte de Siria. Además Turquía siempre ha tenido en mente la idea heredada del imperio otomano de dominar el conjunto del mundo árabe. En ese juego hay una disputa con Arabia Saudí y sus aliados y otra con el Irán chiita (el otro gran credo musulmán), hoy enmascarada por alianzas a corto plazo.

En el escenario futuro se irán viendo de manera progresiva las ambiciones de la India, con un gobierno cada vez más nacionalista, que provocarán crecientes tensiones con Pakistán; se verá el resultado de una iniciativa impulsada por Japón para desarrollar una alianza indo-pacífica que permita contener el expansionismo de China; y se producirá el abandono occidental de Oriente Medio. Con respecto a esto último, ¿quién hubiera podido predecir hace apenas diez años que los principales actores externos de la guerra de Siria iban a ser Rusia, Turquía, Irán y Arabia Saudí, que los Estados Unidos se iban a retirar y que Europa no participaría? Todo esto trae consigo nuevos desafíos, condiciona la política de los Estados Unidos y determina la existencia de alianzas que hoy parecen claras pero que tienen componentes contradictorios. Hay una fuerte alianza entre Rusia y China, dos países que tropiezan en muchos sitios pero que comparten un único objetivo común: debilitar el mundo occidental y la posición estratégica de los Estados Unidos. También hay alianzas entre Rusia y Turquía (enemigos tradicionales) y entre Rusia, Turquía e Irán (no dejan de ser llamativas esas reuniones regulares entre Rohaní, Erdogan

y Putin para discutir sobre el futuro de Oriente Medio y en particular sobre el territorio chino).

Ante estos nuevos desafíos y siguiendo con el símil cinematográfico, Europa podría interpretar un papel de actor de reparto, pero también podría ser un actor secundario o uno de esos actores que aparecen en escenas prescindibles que no afectan al hilo conductor de la película. En realidad, Europa tiene un PIB equiparable al de China o al de los Estados Unidos, tiene suficiente población (a pesar de la evolución demográfica tiene más de cuatrocientos millones de habitantes) y tiene una estructura productiva sofisticada. Pero lo que probablemente le falla es no tener un esfuerzo tecnológico fundamentalmente asociado a la seguridad y a la defensa, a lo que va ligado la inexistencia de un *hard power* europeo real que va íntimamente unido al debate tecnológico y a la necesidad de adaptarse a los nuevos desafíos a los que ya se ha hecho referencia. Europa no dispone de energía, cosa que más o menos se puede resolver. Pero lo que realmente le impide ser un actor de reparto es que no tiene un proyecto ni una idea clara de cuál puede ser su papel en este mundo nuevo. Los Estados Unidos tienen un papel reactivo, pero está claro que saben lo que les conviene aunque a veces no lo parezca. China tiene un proyecto, al igual que Rusia, Turquía e Irán. Pero es muy difícil identificar cuál es el proyecto europeo más allá del *soft power*, y está claro que en este mundo tan agresivo que está abandonando los criterios asociados al orden liberal internacional y en el que el recurso al uso de la fuerza parece menos extraño, si no se tiene *hard power* y autonomía estratégica ligada al desarrollo tecnológico en todos esos terrenos es muy difícil que a un actor se le tenga en consideración.

La ausencia de un proyecto europeo está directamente relacionada con la ausencia de un proyecto político, cosa que sí hubo durante décadas y que ha permitido que la Unión Europea sea un éxito (lo que al mismo tiempo pone de nuevo de relieve esa frase que Felipe González pronunció en otro contexto: «Uno puede morir de éxito»). A la ausencia de proyecto seguramente va también muy asociada la ausencia de liderazgo. Todos los países que se han comentado disponen de liderazgos fuertes en un mundo el que se habla de personas fuertes e instituciones débiles. En el caso de Europa no hay hombres ni mujeres fuertes y las instituciones son cada vez más débiles, porque además de todos

los adversarios externos que condicionan cada vez más su propia existencia se están desarrollando adversarios internos que ponen en cuestión el propio proyecto europeo y buena parte de sus valores, empezando por la democracia o la economía de mercado. Me refiero, lógicamente, a los populismos y a los nacionalismos, que son otra de las grandes amenazas de nuestra seguridad y de nuestra defensa a nivel global.

Pero algo habrá que hacer, porque los desafíos de Europa son ingentes. Habrá que decidir qué tipo de relación se quiere tener con Rusia: únicamente de confrontación, se tiene que basar en imposición de sanciones, se tiene que parar militarmente su amenaza a países occidentales que se sienten coaccionados por sus ansias de expansionismo (empezando por los países bálticos, en los que no es casualidad que haya una presencia española), etc. Habrá que decidir qué actitud hay que tomar frente a China: jugar un papel equidistante en la pugna entre ese país y los Estados Unidos, considerar que puede ser un competidor pero también un socio en ciertas cosas y un aliado en otras, considerarla como un adversario estratégico, etc. Habrá que ver qué decisión se toma con respecto a la inestabilidad política de África del Norte, que nos afecta directamente: Argelia, Túnez, Libia, Egipto y el Sahel, el gran desafío, en donde existen estados incapaces de controlar su propio territorio y en los que tiene presencia el terrorismo internacional.

Habrá que hablar de Oriente Medio y de si Europa puede recuperar el papel que históricamente tuvo y que hoy desde luego no tiene. Habrá que hablar de lo que se debe hacer con Turquía, que por errores europeos y occidentales se está perdiendo. Algo habrá que pensar con respecto a la estabilidad del Mediterráneo Oriental, porque está en juego nuestra seguridad y defensa en el conjunto del Mediterráneo.

Estos desafíos son tremendos y constituyen novedosos retos a la seguridad internacional que afectan específicamente a los europeos. Por ello Europa tiene que repensar radicalmente sus estrategias y ligarlas íntimamente al esfuerzo tecnológico y a la colaboración entre las instancias responsables de su seguridad y defensa, que lógicamente incluyen de manera determinante a nuestras Fuerzas Armadas y a aquellas otras instituciones capaces de generar innovación, desarrollo tecnológico y tecnologías de doble uso que permitan mejorar nuestras condiciones de vida y de defensa.

El mundo va muy rápido. Desde la paz de Westfalia que dio fin a las guerras religiosas en Europa han pasado muchas cosas. Pero Westfalia implicó algo que está desapareciendo: la preeminencia de los estados nación como sujetos activos de la política internacional. Después, tras la derrota de Napoleón vino el Congreso de Viena, cosa que también está quedando muy diluida. Sufrimos las guerras mundiales, caracterizadas por un componente de combate ideológico enormemente fuerte, además del combate militar. Ahora lo que se está viendo es el retorno de la ley de la selva, el retorno al todo vale si eso permite conseguir la hegemonía y ampliar el ámbito de influencia, y el retorno al empleo de todo tipo de recursos aunque no estén desarrollados necesariamente de forma honesta e íntegra. Es el retorno de la geopolítica en su estadio más duro, y por lo tanto el retorno de la famosa frase de Clausewitz «La guerra es la última fase de la política«.

Todo esto da mucho que pensar. Creo que estamos ante un panorama completamente nuevo y completamente inquietante que nos obliga a todos a repensar en nosotros mismos. Porque al final para nosotros, para los europeos occidentales, lo que está en juego es nuestro modelo de sociedad y por lo tanto nuestra manera de entender la libertad y la igualdad.

PANEL II

TOMA DE DECISIONES: INTELIGENCIA ARTIFICIAL Y BIG DATA

Necesidades del Ejército de Tierra

Joaquín Salas Alcalde
General de División Jefe de los Servicios de Información y Telecomunicaciones y Asistencia Técnica del Ejército de Tierra

Vivimos y trabajamos de manera rápida y en constante evolución. Nokia era líder en TIC a finales del siglo xx, las primeras empresas de Ford fracasaron, Disney empezó en el garaje de su casa, Michael Jordan fue apartado del equipo de baloncesto por falta de habilidad y a Edison le dijeron que era demasiado estúpido para aprender cualquier cosa. Esto es evolucionar; o más bien, revolucionar.

Dentro de este entorno de evolución (o revolución) se busca cómo ayudar a cubrir las necesidades del Ejército de Tierra. Hoy en día no tenemos la solución pero no por ello hay que dejar de pensar en buscarla. El impacto de la inteligencia artificial se manifiesta ya en las operaciones de información e influencia. La inteligencia artificial va a disminuir el peligro en las misiones de alto riesgo, la fatiga y la incertidumbre. Y es un hecho que la política militar ya se ve afectada por ciberataques. Hoy disponemos de más datos y de mayor potencia de cálculo pero se está todavía pendiente de un sistema que reflexione por sí mismo. *Big data* es otro concepto que surge de la necesidad de buscar, capturar, analizar y emplear ingentes cantidades de información, pero para salvar vidas lo importante no solo es la cantidad de datos sino su calidad, o sea, la calidad de la información.

Vamos hacia una reducción de los sistemas operativos cerrados, crecen las bases de datos, buscamos una disminución del consumo de potencia y sin duda la simulación va a ser cada vez más vital. Será un reto garantizar que un centro de proceso de datos proporcione una respuesta militar oportuna que permita tomar una decisión militar adecuada. Por ello, la computación deberá ser distribuida y tendremos que aplicar *blockchain* para llegar a la mejor solución. Será esencial el trabajo conjunto de personas y máquinas, pero llegado el momento el mando deberá confiar en las instrucciones y en el asesoramiento de las máquinas, hasta tal

punto que podremos llegar a pensar incluso si llegaremos a delegar funciones en un algoritmo. En los niveles táctico y operacional la inteligencia artificial proporcionará un aumento de capacidades, sobre todo para el conocimiento de la situación. En 2035 habrá ataques de interrupción, interceptación y modificación y fabricación de mensajes falsos, por lo que no va a ser fácil mandar ni mucho menos liderar. Hoy en día podemos pensar que la computación cuántica puede ser la clave que rompa esquemas en 2035, pero puede que por entonces se implante algo todavía más disruptivo y cambie este paradigma. Todo lo que se ha comentado constituye la base teórica reducida de las reflexiones que me han servido para tratar de visionar hacia dónde orientar los esfuerzos de la transformación digital para satisfacer las necesidades de los usuarios del Ejército de Tierra y del conjunto de las Fuerzas Armadas. Hay que tener siempre en cuenta que por mucho que tengamos una visión, cualquier visión sin financiación no deja de ser una alucinación.

La Jefatura de los Servicios de Información y Telecomunicaciones y Asistencia Técnica del Ejército de Tierra (JCISAT) no es un órgano dedicado únicamente a las tecnologías, aunque es lógico que deba conocerlas para poder aplicarlas a los CIS del Ejército de Tierra. También debe conocer la transformación de las operaciones a través del MADOC y debe proporcionar soluciones tecnológicas para apoyarlas. Una parte fundamental de los CIS es la implementación del ciclo de mando y control en sus cuatro fases: conectar, obtener, decidir y actuar. En su visión de Mando y Control 2030, la OTAN pasa del concepto teórico de *network* al concepto práctico de *networking* y resalta la importancia del entorno personas – procesos – tecnologías. Nuestra visión es que la inteligencia artificial es una tecnología transversal que dentro de la Fuerza 35 va a impactar en todas las funciones de combate y a todos los niveles. Algunas de las naciones más relevantes, la OTAN y la Agencia de Defensa Europea ya han empezado a dar pasos en esta línea, considerándola parte de su transversalidad como un valor estratégico cuya finalidad es llegar a proporcionar seguridad en la información.

Las tres tecnologías que actualmente se están estudiando a nivel usuario son la inteligencia artificial aplicada, el *big data* (aplicado sobre todo al uso o a la explotación de datos masivos que provienen de sensores y también de fuentes abiertas) y la

realidad aumentada. Pero para poner en marcha estas tres tecnologías requerimos de una infraestructura que a su vez conlleva la necesidad de nuevas tecnologías o tecnologías emergentes. Desde mi Jefatura estamos contemplando las nuevas arquitecturas de procesamiento, la tecnología cuántica y el 5G (tecnología sobre la que ya estamos haciendo un estudio inicial, a la que consideramos prometedora por su gran ancho de banda y sobre todo por su baja latencia y a la que le vemos aplicación en las redes de sensores). Actualmente se está trabajando en despliegues de redes celulares para los CIS desplegables y se han realizado unas primeras pruebas con 4G desplegando en un entorno operativo para dar comunicaciones seguras a un puesto de mando de nivel brigada. También se está trabajando en el IoT del campo de batalla, concepto que puede ser de gran aplicabilidad a los CIS desplegables (de hecho la OTAN ya ha puesto en marcha iniciativas para la definición de una arquitectura que nos servirá de referencia para engancharnos a ella y seguir adelante), y con el *blockchain*. Además ya está en marcha un estudio aplicado a la seguridad del dato para redes de sensores, porque entendemos y comprendemos que muchos de los datos que provienen de ellos no van a poder ser controlados, y si no hay control de datos no podremos sacar algoritmos fiables para obtener inteligencia.

Cada una de estas tecnologías tiene una misión específica y todas ellas conformarán la arquitectura que definirá los CIS desplegables dentro de la Fuerza 35. Como sabemos, es una tecnología que se va a utilizar en todos y cada uno de los niveles con el objeto de optimizar todos y cada uno de los procesos que se vayan definiendo para identificar y reconocer objetivos, optimizar rendimientos de las comunicaciones y apoyar de manera lógica la toma de decisiones mediante técnicas de apoyo. En este sentido, con el foco puesto en los CIS desplegables se está tratando de emplear inteligencia artificial en la explotación de las redes de sensores y en combinar la inteligencia artificial con el *big data*.

Dentro de la transversalidad y del concepto de nivel estratégico, la Fuerza 35 del Ejército de Tierra utilizará ampliamente la inteligencia artificial en todas y cada una de las funciones de combate. De una forma estratégica, la inteligencia artificial se predispone como clave para todos y cada uno de los elementos que rodean la función mando y control, vertebradora del resto de las funciones de combate.

Entrando más en detalle, hemos identificado cinco grandes funcionalidades o necesidades sobre las que hacemos el mejor seguimiento que podemos. La primera son los agentes inteligentes (sensores). La segunda es la detección de anomalías, que tiene como objeto identificar patrones que hagan que nos equivoquemos lo mínimo posible. La tercera funcionalidad es el conocimiento de la situación (siguiendo la línea marcada por la OTAN). La cuarta, el *sensemaking* para capacidades predictivas. Y la quinta, el apoyo a la decisión (herramientas para buscar alternativas y probabilidades de predecir los efectos negativos que puedan surgir como consecuencia de acciones tomadas que puedan afectar a nuestra decisión).

Dentro de estos estudios generales que hemos puesto en marcha nuestros esfuerzos están dedicados a tres grandes líneas: el apoyo a la decisión, los agentes inteligentes y el *machine learning*. Dentro de estas tres líneas nos hemos centrado en áreas concretas, teniendo en cuenta nuestras limitaciones y nuestras posibilidades y ciñéndonos a lo que el Jefe del Estado Mayor del Ejército de Tierra nos marca en sus directivas y a lo que el propio sentido común determina.

Por lo que respecta a la línea de apoyo a la decisión, nuestro personal técnico está participando en reuniones del grupo de trabajo Data Science de la OTAN. Además se están debatiendo temas específicos sobre la inteligencia artificial relacionados con el mando y control, así como con el diseño, requisitos e integración de equipos efectivos hombre-máquina. También se está impulsando la participación con universidades en el Hackaton OTAN de inteligencia artificial que se desarrollará a principios del próximo año, dentro del triángulo perfecto universidad–empresa–Fuerzas Armadas.

En cuanto a la línea dedicada a los agentes inteligentes, estamos en contacto con la Dirección General de Armamento y Material para trabajar en un proyecto dentro del marco del Programa COINCIDENTE[1] enfocado al desarrollo de sistemas inteligentes

1. El Programa COINCIDENTE (Cooperación en Investigación Científica y Desarrollo en Tecnologías Estratégicas) tiene como principal objetivo aprovechar las tecnologías de carácter civil desarrolladas en el ámbito del Plan Nacional de I+D para incorporar soluciones tecnológicas innovadoras de interés para el Ministerio de Defensa, fomentando así el tejido industrial, científico y tecnológico dedicado a defensa.

(Proyecto Custodes), que va a ser desarrollado por las Universidades de Granada y Jaén y al que se apuntará mi Jefatura para trabajar conjuntamente. La participación en este proyecto nos va a permitir conocer la aplicabilidad de sistemas inteligentes a los CIS desplegables, buscar algoritmos derivados, profundizar en técnicas de *machine learning* y afianzar nuestra relación con las universidades. También dentro de esta línea tenemos una propuesta de la Universidad Politécnica de Madrid (Proyecto MILSCOPE) referente a una plataforma avanzada que posibilite la integración, análisis y visualización de datos dentro de un puesto de mando de brigada en relación directa con los sistemas de mando y control.

Con respecto a la tercera línea, las técnicas de *machine learning* están mostrando ser relevantes para identificar y etiquetar información, por lo que se va avanzando en ese tema. Tenemos prevista la participación en un proyecto de la Organización para la Ciencia y la Tecnología (STO)[2] perteneciente a la Agencia de Defensa Europea de la OTAN. En un principio nuestra participación será a título de observadores, lo que nos permitirá profundizar en el estado del arte de estos asuntos relacionados.

En la primera jornada de la Academia de las Ciencias y Artes Militares celebrada en Madrid el pasado 3 de octubre se habló del repóquer disruptivo de hoy en día, compuesto por *big data, machine learning*, inteligencia artificial, computación cuántica y *blockchain*. También de que el conflicto de alta intensidad puede ser *hard* o *soft*: el *hard* se centrará más en la infraestructura mientras que el *soft* irá más enfocado a la infoestructura (a ese 65% de la población que se concentrará en ciudades, de la cual el 70% será marginal). En cuanto a las tendencias de inteligencia artificial se mencionó que son tan variadas que se queda corto un trozo de papel para enumerarlas. En cuanto a la obtención de tecnologías disruptivas se expuso la necesidad de cambiar el paradigma que hace que sea más largo el proceso de obtención que el ciclo de vida de los elementos que se obtienen. Y por último se dijo que las tecnologías hoy en día no son impedimento para sacar un proyecto adelante y conseguir un objetivo operativo.

2. Organización para la ciencia y la tecnología (*Science and Technology Organization*).

En la JCISAT estamos trabajando en tecnologías que puedan ser aplicables en un ámbito general y más concretamente en el de los CIS desplegables. El repóquer disruptivo es estratégico por su transversalidad. Recomendamos aprovechar el impulso de las muchas instituciones que ya han empezado a trabajar en este asunto. Focalizamos el esfuerzo en el apoyo a la decisión, en los sensores y en el *machine learning*. Abrimos líneas de trabajo para aquellos grupos que ya están constituidos y para aquellos proyectos que están en visos de constituirse. Y lógicamente, toda esta participación nos va a permitir acercarnos al uso de estas tecnologías con un único objetivo: llegar a obtener productos para la Fuerza 35.

Capacidades de la Universidad de Granada

Francisco Herrera Triguero
Catedrático del Departamento de Ciencias de la Computación de Inteligencia Artificial de la Universidad de Granada

La inteligencia artificial es una disciplina relativamente joven. El término inteligencia artificial fue propuesto por John McCarthy en el año 1955 con ocasión de un primer congreso en el que los investigadores más relevantes de los Estados Unidos se reunieron para hablar de esta disciplina. McCarthy se refirió entonces a la inteligencia artificial como «La ciencia e ingeniería de hacer máquinas que se comporten de una forma que llamaríamos inteligente si el humano tuviese ese comportamiento», siendo esta una definición que aún se emplea en nuestros días. Es decir, que estamos hablando de tecnologías que emulen el comportamiento humano de manera inteligente.

Me voy a centrar muy brevemente en tres hitos de los últimos veinticinco años para saber dónde estamos ahora mismo y también en la fusión de inteligencia artificial y *big data*. El primer hito está datado entre los años 1996 y 1997. IBM creó Deep Blue, un sistema inteligente para jugar al ajedrez que en 1996 consiguió ganar una partida al entonces campeón del mundo Gary Kaspárov y que un año después, con un sistema renovado, fue capaz de ganar el torneo realizando algunas jugadas que generaron asombro en aquel entonces. El segundo hito se produjo en 2005, año en el que un coche autónomo con sistemas inteligentes que aprendían de la experiencia (de los datos) fue capaz de cruzar desiertos y bosques para llegar por primera vez a la meta del DARPA Grand Challenge, lo que constituyó el primer gran reto que el *machine learning* consiguió alcanzar. Y el último hito ocurrió en 2016, año en que DeepMind Technologies consiguió fabricar un sistema inteligente denominado AlphaGo que fue capaz de ganar a Lee Sedol, campeón del mundo de Go (juego de estrategia más complejo que el ajedrez), por un resultado de cuatro a uno. De las cinco partidas que se disputaron Lee ganó únicamente la primera,

por lo que se demostró que era posible diseñar un sistema inteligente que a la vez aprendiese de la experiencia.

Esto nos situó en lo que hoy llamamos la era del *big data*, la era de los datos masivos, una era en la cada treinta minutos estamos generando más de cincuenta *petabytes* de información (el equivalente a todos los trabajos escritos en la historia de la humanidad en cualquier lengua) y aproximadamente cada dos años estamos doblando la cantidad de información que vamos generando en todo el planeta.

Esto nos sitúa en un mundo en el que estamos fusionando la inteligencia artificial y el *big data*. Realmente cuando hablamos de *big data* hablamos de inteligencia artificial. Estamos hablando del procesamiento de una cantidad masiva de datos que requiere de los algoritmos de *machine learning* para poder procesarlos y extraer conocimiento. Podemos decir que la inteligencia artificial multiplica exponencialmente la capacidad de la analítica de datos. No podemos hablar de *big data* sin inteligencia artificial, porque la inteligencia artificial moderna utiliza los datos para extraer conocimiento y resolver problemas.

Estamos en una era en la que podemos hablar de máquinas no pensantes que son cada vez más capaces. Como decía Rouhianinen[1] «El mundo cambiará gracias al crecimiento de la inteligencia artificial». Igualmente, Yuval Noah Harari[2] en la presentación de su libro Homo Deus (en el que habla del dataísmo) mencionó que «El mundo va a cambiar radicalmente gracias a los algoritmos, el *big data* y la inteligencia artificial». Y no solo va a cambiar sino que está cambiando. Actualmente hay estudios que nos dicen que el 65% de los niños que comienzan la educación primaria van a trabajar en profesiones que hoy no existen y que va a haber una automatización y transformación total de la sociedad tal y como la conocemos hoy en día.

Se ha hablado de la importancia que tienen los Estados Unidos y China a nivel tecnológico y a nivel de inteligencia artificial. Pero Europa también tiene sus fortalezas y un gran potencial.

1. Escritor, consultor y experto internacional en inteligencia artificial, tecnologías disruptivas y marketing digital. Es uno de los divulgadores más importantes en Europa.

2. Historiador y escritor israelí, además es profesor en la Universidad Hebrea de Jerusalén.

Según un estudio realizado por Roland Berger[3], España está actualmente en el grupo de cabeza de Europa en cuanto a potencial en inteligencia artificial (concretamente España es la cuarta potencia). Para la realización de este estudio la consultora tuvo en cuenta no solo centros de investigación y universidades sino también *startups* y empresas. Por lo tanto, España está en una buena situación de partida, con un potencial en inteligencia artificial que está a la altura de cualquier país europeo, lo que permite abordar cualquier proyecto que nos planteemos.

El un estudio de THE publicado en 2017 en el que se analiza la productividad científica entre 2011 y 2015, España figura a la cabeza de los países europeos al mismo nivel que Francia y por detrás de Alemania (excluido ya el Reino Unido). En el estudio se analizó no solo la cantidad de producción científica sino su calidad, medida en términos de veces que las publicaciones han sido citadas por investigadores de otros centros. En esta clasificación la Universidad de Granada ocupaba la cuarta posición mundial. Obviamente, cada *ranking* tiene en consideración unos factores determinados y en función de ellos se puede estar en una u otra posición. Pero lo cierto es que en cualquier estudio internacional que se hace en inteligencia artificial la Universidad de Granada siempre ocupa un puesto de relevancia (que podemos situar entre el *top* 20 y el *top* 30). En reconocimiento a esta notabilidad de nuestra Universidad, el Presidente del Gobierno de España y el Ministro de Ciencia presentaron en Granada la Estrategia de I+D+i de Inteligencia Artificial, en la cual, por cierto, participaron algunos de nuestros investigadores.

La Universidad de Granada dispone de un Departamento de Ciencias de la Computación e Inteligencia Artificial en el que trabajan setenta personas de manera permanente y que da servicio a alrededor de ciento cincuenta investigadores (contando postdoctorados, doctorandos y profesores docentes). Este Departamento desarrolla su investigación en torno a nueve grupos de investigación y se podría decir que a su cargo está el 70% u 80% de la producción científica que se realiza en la Universidad.

También dispone de un Centro de Investigación en Tecnologías de la Información y las Comunicaciones, centro de referencia

3. Consultoría estratégica a nivel mundial con sede central en Múnich.

a nivel europeo en TIC que engloba toda la investigación que se hace en este ámbito, con laboratorios al más alto nivel en nanotecnología, 5G, distintas áreas de inteligencia artificial, etc.

Y recientemente la Junta de Andalucía publicó la creación del Instituto Andaluz Interuniversitario en Data Science and Computational Intelligence (DaSCI)[4], nacido de un acuerdo entre la Universidad de Jaén y la Universidad de Granada al que se incorporará la Universidad de Córdoba en los próximos meses. Este instituto se ha creado en torno a tres grandes áreas: la ciencia de datos (*machine learning* y *big data*), la inteligencia computacional y las diferentes técnicas de optimización (sistemas inteligentes con una especial atención a las aplicaciones en lo que se podría denominar sociedades y economías digitales, con aplicaciones en múltiples áreas). Actualmente tiene proyectos abiertos en el ámbito aplicado con empresas y en el ámbito de energía, seguridad, industria 4.0, turismo y tecnologías virtuales, así como con el Programa COINCIDENTE. Ha sido, junto a la Universidad de Granada, el impulsor de la plataforma de transferencia de inteligencia artificial en Andalucía. En esta Comunidad se ha creado el Digital Innovation Hubs DaSCI (DIH DaSCI)[5] con la participación de las Universidades de Granada (coordinadora), Jaén, Córdoba, Huelva y Cádiz más un conjunto de empresas. Este DIH nace con vocación de ser una de las herramientas de transferencia de la inteligencia artificial a nivel andaluz en todos los sectores industriales.

Algunos proyectos de investigación actualmente en curso son el Copkit[6] (proyecto de María José Martín Bautista, catedrática del Departamento de Ciencias de la Computación) y el Proficient[7] (proyecto del doctor Juan Gómez-Romero, un joven investigador que se ha incorporado recientemente al Departamento, muy bien valorado por su gran potencial en el desarrollo de sistemas inteligentes que permitan grandes ahorros en consumo energético).

4. Ciencia de Datos e Inteligencia Computacional.

5. Centros de innovación digital DaSCI.

6. Proyecto europeo en el ámbito de la seguridad con la idea de detección de amenazas y el diseño de alarmas tempranas. Se centra en el problema de analizar, investigar, mitigar y prevenir el uso de nuevas tecnologías de información y comunicación por parte del crimen organizado y los grupos terroristas.

7. Tiene como objetivo mejorar la eficiencia energética y adaptar el funcionamiento de determinados equipos a la demanda de energía, minimizando el consumo y manteniendo cómodos a los ocupantes de un edificio.

El Instituto también está desarrollando dos proyectos en el ámbito de la seguridad. El primero se realiza en colaboración con la empresa andaluza de seguridad Ontech Security, con la que se han desarrollado herramientas inteligentes que a partir de la elaboración de un campo magnético permiten controlar el paso a través de puertas. El segundo tiene que ver con la detección inmediata de objetos tales como armas, a la que puede ir asociada la activación de un sistema de alarma en tiempo real. Esta línea de investigación se está desarrollando con tecnologías de *deep learning* en colaboración con la Universidad de Jaén.

Y para terminar, mencionar el Proyecto Custodes del Instituto DaSCI. Este es el primer proyecto en el ámbito puramente de defensa, con el que pretendemos desarrollar un sistema inteligente que permita procesar imágenes y detectar amenazas en un escenario de conflicto empleando tecnologías de *deep learning*. Quiero agradecer públicamente al MADOC todo el apoyo que ha prestado y presta para impulsar este proyecto así como a la empresa doIT, sin cuyo trabajo de coordinación el proyecto habría sido imposible. Gracias también a la Universidad de Jaén, personalizadas en la investigadora principal del proyecto (la catedrática María José de Jesús) y gracias al grupo de la Universidad de Granada que tengo el honor de dirigir.

Por último, recordar que cuando hablamos de inteligencia artificial estamos hablando de máquinas no pensantes pero cada vez más capaces. Un artículo reciente sobre inteligencia artificial cuestionaba si la afirmación de que una máquina no puede crear se podría considerar mito o realidad. Ahí queda esa pregunta, porque cada vez más las máquinas inteligentes están en disposición de crear.

Capacidades tecnológicas

Sebastián Laiseca Segura
Departamento de Tecnologías Avanzadas para Defensa de Indra

La toma de decisión es una de las mayores responsabilidades que tiene un militar y una buena forma de enfocar este tema desde el punto de vista tecnológico es usar un *framework*. El más conocido que puede servir de base es el relacionado con el concepto de consciencia situacional. La consciencia situacional fue presentada en las fuerzas aéreas estadounidenses en 1995 por M. Endsley[1], quien dejó claro cuáles son los tres puntos críticos que se deben tener en cuenta para tomar una decisión: la percepción, la comprensión y la proyección. Esos son los tres puntos clave con los que trabajamos en Indra, puntos que hemos expandido para construir lo que llamamos la Pirámide de la consciencia situacional para la ayuda a la toma de decisión (figura 1). En el *framework* original de 1995 la parte de decisión se situaba fuera del concepto de consciencia situacional. En Indra lo hemos incluido, y veremos por qué.

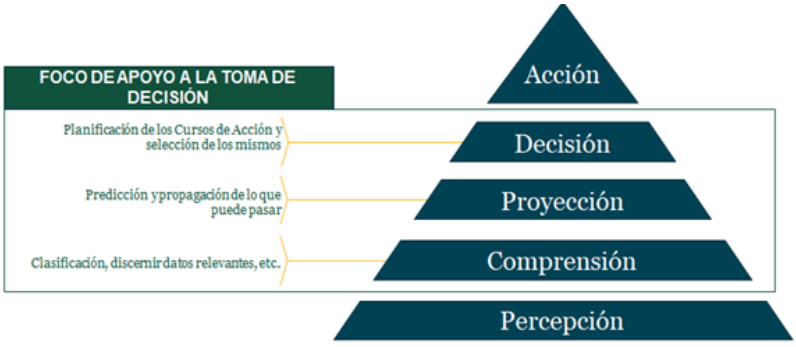


Figura 1. Pirámide de la consciencia situacional

1. Ingeniera y ex científica jefa de la Fuerza Aérea de los Estados Unidos.

Lo primero que debemos entender es que para tomar decisiones necesitamos información. A esta primera etapa la hemos llamado percepción. La percepción es simplemente una recopilación de información de diferentes fuentes, que pueden ser informáticas, de inteligencia o provenir de puestos avanzados de mando. Este punto es el más clave de todos, ya que si falla, el resto del proceso de toma de decisión va a suponer un problema.

Una vez que tenemos toda la información, la siguiente etapa que definimos es la comprensión: tenemos que dar sentido los datos que tenemos (simplemente entenderlos). En este caso podemos hablar de clasificación de datos. Cuando se habla de *big data* ocurre que en muchas ocasiones el simple hecho de disponer de tanta información hace que no se use porque no se sabe muy bien cuáles son los datos a utilizar. Un ejemplo de comprensión de datos podría ser la identificación de objetos a partir de imágenes.

Una vez que comprendemos lo que está sucediendo, pasamos a la etapa de proyección aplicando las tecnologías adecuadas. La proyección tiene una importancia completamente diferente a la comprensión. Por poner un ejemplo, un coche autónomo puede detectar perfectamente peatones en la calle pero tiene que saber proyectar, es decir, tiene que saber que un viandante que se dirige hacia un paso de peatones tiene la intención de cruzar. El poder proyectar, y más en el ámbito de defensa (para conocer la intención de un potencial adversario), es fundamental.

Una vez estudiadas todas las opciones en la fase de proyección, corresponde la toma de decisión y la planificación del curso de acción. En este ámbito también se están aplicando muchas técnicas de inteligencia artificial. La más común y conocida se basa en simples árboles de decisión en el que los pesos dinámicos van cambiando en función del resto de elementos.

En Indra, el foco del apoyo a la toma de decisión lo centramos en tres pilares: comprensión, proyección y decisión. Separándolos bien y pudiendo segmentar claramente dónde empieza cada uno se pueden obtener soluciones completamente modulares que pueden hacer que seamos capaces de planificar para el futuro y cambiar los componentes a medida que se vayan mejorando merced a la aceleración tecnológica.

A continuación explicaré un ejemplo real que está ligado al tema de la consciencia situacional aplicada al ciberespacio y cómo se puede aplicar la Pirámide a las operaciones militares. En este

caso nos centramos en un sistema de ciberconsciencia situacional (consciencia situacional aplicada al ciberespacio). Lo primero que se haría en un sistema de ciberconsciencia situacional sería detectar y percibir lo que está pasando a nivel de servicio mediante sistemas físicos informáticos (CIS). El siguiente paso sería comprender, es decir, enterarse de lo que está pasando a través de toda la información que se está captando. El tercer paso sería proyectar, pero aquí es donde empieza la complicación. Cuando hablamos de proyectar la información CIS que estamos recopilando, realmente lo que interesa es saber cómo va a impactar esta información en la misión en curso, y es entonces cuando comienzan las complicaciones de las traslaciones. Lo importante es saber y ser capaz de trasladar a la capa de visión un riesgo o un evento detectado en el nivel CIS y ver no solo cómo se proyecta a ese nivel sino cómo va a impactar el riesgo en la misión a largo, medio o corto plazo.

Una vez tenemos las proyecciones corresponde decidir, pero la decisión se haría en sentido inverso: se decidiría en función de lo que fuese mejor para la misión y esa decisión se aplicaría a nivel CIS.

Esta traslación de dimensiones se puede apreciar si descomponemos una misión en niveles CIS. Para comprenderlo, vamos a hacerlo tomando como ejemplo el proyecto que estamos llevando a cabo con la Agencia de Defensa Europea, que cuenta con la participación del Mando Conjunto de Ciberdefensa de España. En este proyecto estamos desarrollando una metodología que sea capaz de transferir al nivel de la misión lo que está pasando a nivel CIS. En este caso, el primer nivel sería la capa de nivel CIS más básico (la capa física *hardware*); el segundo nivel serían los servicios de nivel CIS (servicios generales que se utilizan típicamente a nivel CIS); el tercer nivel sería el *business process*[2] que define los bloques de una misión; y el cuarto y último nivel sería el de objetivos de la misión en curso.

Pero como es sabido, para toda acción hay una reacción igual y opuesta, lo que no es específico de las nuevas tecnologías. Desde

2. Proceso de negocio o método de negocio. Es una colección de actividades o tareas relacionadas y estructuradas que, en una secuencia específica, produce un servicio o producto para un cliente o clientes concretos.

que hay castillos y murallas hay arietes y escaleras, en un juego continuo de ver cómo nos podemos defender. Cuando hablamos de toma de decisión, inteligencia artificial y Ejército lo interesante es saber qué tipo de ataques pueden hacer contra nuestros sistemas. Podríamos pensar en uno que inhabilitase un sistema entero, pero tal vez sea peor uno que nos haga pensar que el sistema está funcionando correctamente cuando en realidad no lo está haciendo. Hay ejemplos que demuestran que con una simple modificación de una imagen un sistema de inteligencia artificial no es capaz de seguir razonando (lo que hacen es atacar al primer elemento de la pirámide, la percepción, con lo que todo el resto se tambalea). Pensemos en un coche autónomo, el cual tiene que ser capaz de detectar diferentes tipos de objetos y a cada uno tratarlo de una forma diferente. El coche puede detectar a un ciclista al identificar perfectamente su bicicleta y debe actuar teniendo en cuenta que su comportamiento es mucho más impredecible que el de un coche (figura 2).

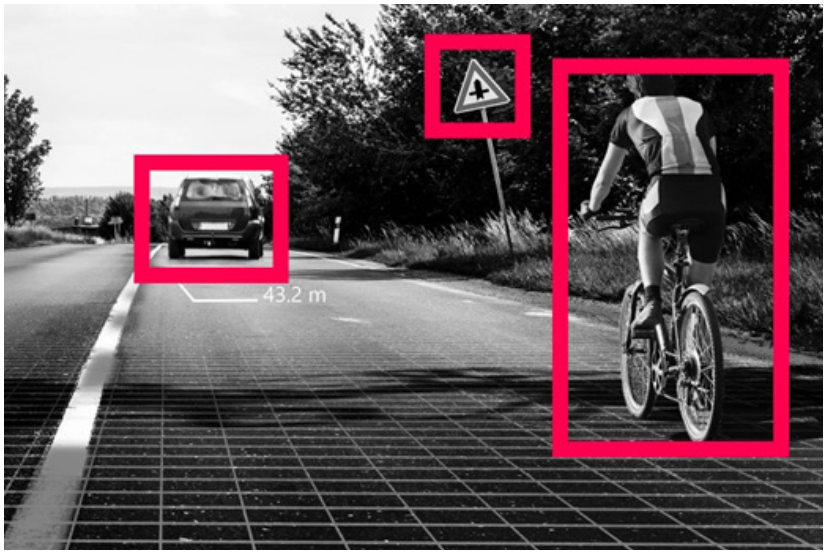


Figura 2. Posible identificación de objetos de un vehículo autónomo

Pero, ¿qué sucede cuando el sistema del coche detecta una bicicleta en un portabicicletas de otro coche? (figura 3).

Figura 3. Bicicleta sobre portabicicletas de un vehículo

En este caso puede que sea sencillo, porque el sistema es capaz de darse cuenta de que la bicicleta siempre está en horizontal y por lo tanto no tiene que prestarle atención. Pero cuando el sistema capta la imagen a tamaño real de un ciclista en la publicidad trasera de un autobús comienzan los problemas (figura 4).

Figura 4. Publicidad de un ciclista sobre un autobús urbano

Al reconocer este tipo de imagen, ciertos coches autónomos se volvían un poco locos porque no entendían bien lo que sucedía y no sabían cómo reaccionar. Nos podemos imaginar las consecuencias que puede tener esto en un campo de batalla. Si nuestro reconocimiento del enemigo se basase exclusivamente en imágenes o en detección de objetos sería demasiado trivial y demasiado fácil para el adversario imprimir imágenes y hacernos pensar que tiene más de lo que realmente tiene.

En muchas ocasiones la inteligencia artificial nos sorprende (un ejemplo ha sido la derrota de Kaspárov por Deep Blue). Comentaré dos ejemplos reales para comprender lo difícil que es ver por dónde va a salir la solución de la inteligencia artificial y que tenemos que tener claro que la mejor solución puede ser una que ni siquiera habíamos tenido en cuenta. En un primer ejemplo, (figura 5), unos investigadores estaban intentando optimizar el movimiento de un robot de seis patas de forma que estas estuviesen en contacto con el suelo el mínimo tiempo posible en términos de porcentaje para que pudiese andar por un terreno caliente o peligroso. Para asombro de todos, el robot decidió que la mejor forma era darse la vuelta y andar al revés. Realmente cumplió con todas las premisas y no solo consiguió reducir el porcentaje de contacto de las patas con el suelo, sino que lo redujo a cero.

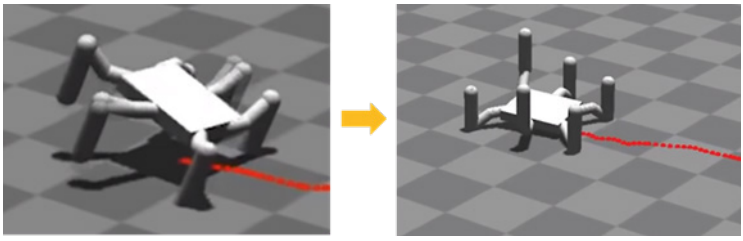


Figura 5. Ejemplo de comportamiento de robot entrenado con inteligencia artificial de forma autónoma

En cuanto al segundo ejemplo, unos investigadores intentaron enseñarle a un robot a andar por sí solo. Se colocó al robot a una distancia equivalente a la medida de su cuerpo con respecto a una línea de meta y se le indicó que la alcanzase de la forma más rápida. El robot, después de muchas simulaciones, se dejó caer al suelo y cumplió de este modo su objetivo. Estos dos ejemplos demuestran que la definición de las reglas que se le dan a los sistemas de inteligencia artificial son tan importantes o más

que la propia algoritmia y que por eso es muy importante tener el control.

Todo el mundo sabe que Google es una eminencia en temas de detección y clasificación de imágenes con inteligencia artificial. Con esta compañía se hizo la siguiente prueba: a una simple imagen de un panda que Google fue capaz de interpretar con una confianza de un 60% se le añadió ruido blanco (una imagen totalmente imperceptible al ojo humano), a raíz de lo cual Google interpretó la imagen de un mono (figura 6).

Figura 6. Resultados de Ian J. Goodfellow et al, Explaining and Harnessing Aversarial Examples (2015)

Podemos imaginar que esto tiene unas consecuencias muy importantes para los sistemas de defensa, los cuales pueden llegar a interpretar cualquier cosa diferente a la imagen que tienen delante si el adversario le ha añadido algún tipo de ruido (figura 7).

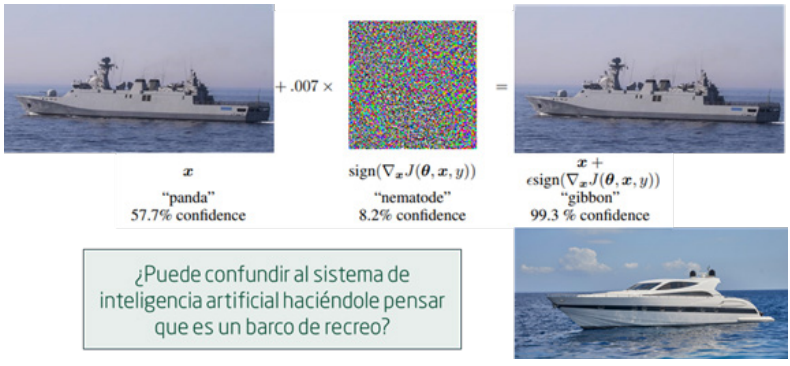


Figura 7. Simulación de introducción de ruido blanco a una imagen de una fragata

Por eso cuando se habla de inteligencia artificial es tan importante la parte ciber, la guerra electrónica y sobre todo su convergencia. Esto es claramente un *known unknown*[3] en el sistema anglosajón: no sabemos cómo nos van a atacar ni cómo un potencial adversario va a poder aprovecharse de estos sistemas e intentar hacer un ataque.

Lo que estamos haciendo en los sistemas de ciberconsciencia situacional que estamos desarrollando en Indra para el Mando Conjunto es asegurarnos de que todos los módulos y todos los subsistemas se puedan reemplazar y se puedan cambiar uno a uno. Ya no trabajamos con la idea de que un sistema va a ser funcional durante quince o veinte años tal y como lo conocemos, seguramente en los próximos cinco o diez años se lleven a cabo actualizaciones muy importantes. Estamos diseñando sabiendo que el mundo cambia de manera acelerada y sabiendo que ciertos componentes deberán ser reemplazados más pronto que tarde. Estamos diseñando sabiendo que hay amenazas que todavía ni nos podemos imaginar, por lo que cada cierto tiempo nos reunimos e intentamos ver cómo se podría atacar determinado sistema. Y lo más importante, estamos trabajando en colaboración con las universidades y las Fuerzas Armadas y al mismo tiempo estamos buscando colaboradores o asociados en cada etapa de ayuda a la toma de decisión.

3. Conocido sin conocer, es algo que no sabemos y por lo tanto sabemos que no lo sabemos.

Enfoque humanista

Francisco José Hernández Guerrero
Fiscal de la Fiscalía Provincial de Granada

Hasta ahora se ha tratado la inteligencia artificial desde un aspecto mecánico. En este sentido los logros que se pueden conseguir por la Universidad de Granada son absolutamente punteros. Pero surge una pregunta: ¿realmente queremos tanta inteligencia artificial en nuestra vida? ¿Somos conscientes de los cambios que introduce la inteligencia artificial en nuestra forma de vivir y en nuestro estatuto de derechos como ciudadanos? Voy a poner unos ejemplos que se han producido durante los años 2016 y 2017 en materia de inteligencia artificial, sobre todo en proyectos relacionados con lenguaje natural.

El primero de ellos tiene que ver con los famosos *bots* elaborados por Google, Facebook y Microsoft. Google puso en marcha varios sistemas de *chatbots* entre diversas redes neuronales para ver cómo funcionaban. En un sistema denominado Bob, Alice y Eva, Bob le tenía que mandar un mensaje a Alice y Eva tenía que interceptarlo. De manera inesperada Bob y Alice diseñaron un sistema de cifrado natural muy simple y rudimentario que hizo que Eva no se enterara absolutamente de nada. Esto sorprendió mucho a los autores del experimento, pues no se esperaban que fueran tan creativos (no tenemos que preocuparnos, no pasa nada estamos lejos de Skynet[1]).

Facebook puso en marcha otro experimento, también con los nombres de Bob y Alice. Bob y Alice Facebook estaban hablando en lenguaje natural, concretamente en inglés, y se dieron cuenta

1. Es el nombre que recibe la inteligencia artificial que lidera al ejército de las máquinas en la saga de películas Terminator, y es el principal antagonista de ésta. En la saga, Skynet es una inteligencia artificial capaz de controlar el arsenal militar de los Estados Unidos con independencia de los humanos.

que era mejor hablar en un dialecto que ellos mismos se inventaron porque la cosa iba más rápida. La noticia fue espectacular. Una vez que se aclararon las instrucciones se averiguó que lo que se estaban diciendo era bastante sencillo, pues simplemente comentaban que habían encontrado un método más eficiente para desarrollar su labor.

Más interesante aún fue el experimento de traducción que hizo Google Brain a través de Google Translator. Le dieron los parámetros para realizar una traducción del portugués al inglés y del inglés al español. Y la máquina aprendió a traducir del portugués al español directamente. Efectivamente, las máquinas son muy capaces pero todavía no son pensantes. Estos ejemplos nos llevan a pensar que no se sabe hasta dónde vamos a avanzar y si vamos a tener que correr algún riesgo o no.

Microsoft hizo otro experimento que a mí me resulta mucho más interesante. Crearon una *chatbot*, a la que pusieron de nombre Tyde, para controlar y moderar un chat de adolescentes. Entre los adolescentes se introdujo un grupo llamado Forchange que se dedicaba al *hacking* lúdico: entraron en el correo electrónico de Sarah Palin (gobernadora de Alaska, ultra conservadora) para demostrar que podían entrar en cualquier sitio. Y lo que hicieron fue saturar el sistema con mensajes de odio y discriminatorios hasta que el sistema, por su estadística y sesgo, aprendió el lenguaje mayoritario del grupo y acabó insultando, siendo neonazi y extremadamente violento. De ahí pasó a las mazmorras cibernéticas y nunca más se supo de ella.

Las inteligencias artificiales, efectivamente, necesitan un enfoque ético. El ADN de la Unión Europea es el enfoque ético y la protección de los derechos humanos y ello lleva a que cualquier sistema de inteligencia artificial que se aplique tiene que cumplir determinados parámetros de protección de los derechos humanos, como son fiabilidad, transparencia, control humano (la inteligencia artificial o incluso el robot más avanzado deben tener un control humano final, no pueden ser absolutamente autónomos) y no discriminatorio. El problema es que la discriminación se puede producir al revés. El algoritmo puede ser perfecto, pero los humanos pueden modificarlo cambiando las bases (por ejemplo, aumentando los datos incorrectos de los cuales se va a alimentar ese *big data*) de modo que el algoritmo, que es correcto en su funcionamiento, ofrezca unas soluciones extrañas. Los políticos sa-

ben esto muy bien y lo usan en lo que llaman política automática: generan muchos perfiles en internet que retuitean sus mensajes para crear mucha más recepción y para proponer y proyectar un discurso que puede ser contra el adversario o propagandístico del suyo propio; pero en el fondo lo que hacen es manipular el *big data* a su favor: el algoritmo funciona correctamente pero la base de la aplicación es incorrecta. Esa es la situación actual. La Unión Europea pretende dar ese enfoque de fiabilidad, de responsabilidad, de conservación del entorno ambiental y de usar fuentes certificadas para que esas bases de información sobre la que tiene que operar la inteligencia artificial sean correctas.

En cuanto a la aplicación de los sistemas de inteligencia artificial en el mundo de la justicia, se plantea también el tema de cómo deben ser los algoritmos que se generen. En diciembre de 2018 el Consejo de Europa dictó una Carta Europea de Uso de la Inteligencia Artificial en Sistemas Judiciales en la que se establecen más o menos los mismos principios, es decir, ese enfoque ético, esa necesidad de protección y de ética en el diseño de las aplicaciones y de los algoritmos de inteligencia artificial. Esto también está recogido en nuestra Estrategia de Inteligencia Artificial e I+D, pero personalmente no sé si somos realmente conscientes de lo que va suponer sustituir, o al menos introducir, inteligencias artificiales dentro del proceso judicial.

Precisamente esta preocupación por el efecto que pueden tener las inteligencias artificiales en la valoración del comportamiento de los seres humanos está dando lugar a una serie de normas reguladoras que están estableciendo una serie de derechos informacionales de segundo nivel (los derechos informacionales de primer nivel serían los famosos ARCO: Acceso, Rectificación, Cancelación y Oposición). Concretamente el artículo 22 del Reglamento General de Protección de Datos, establecido por el Reglamento 679/2016 del 22 de abril, base de nuestra regularización sobre protección de datos en el ámbito europeo, establece el derecho a no verse sometido a una decisión automatizada, a ser informado de la lógica del sistema o del proceso decisorio y a tener derecho a una intervención humana en el proceso de decisión. Es decir, se ha introducido por esa vía lo que para mí es lo más importante de todo el reglamento: el hecho de que frente a las inteligencias artificiales está el derecho de un ser humano a ser juzgado por otro ser humano, no por una máquina ni por

un algoritmo por muy inteligente que sea. En 1997 discutía sobre el derecho al error que tenemos como seres humanos. Personalmente, si soy procesado quiero que me juzgue un ser humano, porque el ser humano puede que tenga un sesgo de emoción, de correlación y de empatía que quizás la máquina no tenga, y tengo derecho a esa naturaleza humana aplicada al juicio sobre mi vida.

La introducción de algoritmos en el proceso va a generar un cambio de los derechos que tenemos como justiciables ante los tribunales de justicia. Por ejemplo, va a cambiar el derecho de defensa. Si una máquina se puede entender con otra máquina, la máquina de mi abogado se puede entender con el sistema de decisión judicial y la máquina judicial del sistema experto puede analizar su contenido, escanearlo, contextualizarlo, obtener los ítems importantes para la decisión y resolver, ¿para qué van a servir los abogados? Los abogados se convertirán en abogados de oficio. ¿Cómo se va a resolver eso? ¿Dónde va a quedar la labor del abogado? En la argumentación desde luego que no, puesto que no habrá argumentación ni retórica ya que no se necesitará convencer a las máquinas. El algoritmo necesita documentos, extraer los datos esenciales y aplicarles las reglas de decisión. La retórica, la argumentación, no sirve de nada. A lo mejor queda el dato creativo: el abogado tendrá que emplear la creatividad para argumentar que determinado algoritmo no se puede aplicar a determinado proceso o a determinado supuesto porque no ha sido creado para ello. Tanto el abogado como la parte fiscal tendrán que ser muy creativos. Por ejemplo, en un procedimiento de intoxicación por contaminación alimentaria en el que participé, en el que las pruebas por las que todo un barrio fue al hospital por culpa de una intoxicación alimentaria estaban claras, la defensa del letrado cuestionó el resultado de los análisis porque el microscopio que se empleó para realizarlos no estaba homologado. *In dubio pro reo*, no podemos estar seguros, procedimiento ganado. Cuestionó el sistema en la parte más elemental. Esa va a ser la labor creativa del abogado.

Y si esto es así, ¿vamos a poder predecir, por ejemplo, el comportamiento del juez? ¿Voy a poder aplicar el *big data* y analizar todas las resoluciones judiciales de Manuel Marchena[2], por ejemplo?

2. Jurista español, magistrado del Tribunal Supremo desde 2007, actual presidente de la Sala Segunda de lo Penal.

Es decir, voy a ver cómo piensa Manuel Marchena en determinados tipos de procedimientos, voy a ver si me interesa o no, voy a aplicar las normas y voy a intentar predecir qué va a plantear o cómo va a resolver mi caso. ¿Es legítimo que yo use el sesgo (la decisión automatizada) en el sentido inverso, es decir, no que yo me someta a una decisión automatiza sino que yo someta a una decisión automatizada a quien me va a juzgar? ¿Rompe las garantías procesales? ¿Tiene derecho el justiciable a ser más poderoso que el poder judicial de Estado que le tiene que juzgar? En Francia lo tienen claro: en 2016 se determinó que eso era un delito. Una ley que modifica el Código Penal estableció que eso está sancionado con hasta cinco años de prisión. De este modo, los sistemas de Legal TIC, por ejemplo, se van al traste: no se pueden usar los nombres y apellidos de los magistrados de una sala para intentar predecir cuáles son sus resultados. Personalmente no tengo tan claro que eso no se pueda hacer porque actualmente lo estamos haciendo en plan manual: analizamos las sentencias, intentamos saber cuáles son los sesgos ideológicos de los magistrados y presentamos un tipo de recurso u otro o un tipo de argumentación u otra.

Pero realmente la defensa también va a cambiar mucho en otros aspectos. Por ejemplo, se habla mucho de los sesgos de los algoritmos. ¿Se ha pensado en los sesgos positivos que tiene el sistema de justicia? Por ejemplo, la presunción de inocencia es un sesgo a favor del reo: el estado no puede sancionar a una persona sin pruebas y sin una mínima capacidad probatoria de signo incriminatorio. Eso es un sesgo, una regla de determinación. *In dubio pro reo* obliga a que, si no hay pruebas, en caso de duda se debe beneficiar al reo. Es una forma de compensar al indefenso frente al estado. Si decimos que las máquinas no deben tener sesgo, ¿queremos algunos sesgos positivos como este? O, por ejemplo, ¿cómo protegemos a un consumidor frente a una gran multinacional con el sistema de inversiones de carga de prueba? ¿Vamos a permitir que el algoritmo detecte esos elementos y esos factores y los aplique o vamos a dejar que esa ponderación, ese ajuste fino, esa búsqueda de la justicia en un caso concreto, lo haga el magistrado de instancia? Si la primera resolución judicial la dicta un algoritmo, no vamos a tener esa capacidad creativa. Como además lo realiza de una forma automatizada, no va a ser necesario motivar la sentencia: ya sabemos que esta automatizado y está objetivada, luego hemos aceptado legalmente esa decisión.

¿Y qué ocurre en vía de recurso? ¿Qué van a hacer los tribunales supremos y el Tribunal Superior de Justicia? Puede que establecer los sesgos favorables al individuo, establecer las líneas creativas que van a permitir modificar y mejorar los algoritmos y/o ajustarlos a casos concretos. El papel de los recursos va a cambiar, el papel de los tribunales de segunda instancia va a cambiar, el papel de las motivaciones y de las resoluciones judiciales va a cambiar y el peso de las pruebas de los procesos va a cambiar: no se tratará de acreditar los hechos sino de verificar que las valoraciones que realice la máquina sean absolutamente correctas (que el algoritmo sea el correcto).

¿Cuáles son los problemas a los que nos vamos a enfrentar? Por ejemplo, en materia penal ya estamos viendo una aplicación concreta que está empleando inteligencia artificial muy básica para la evaluación de riesgos. VioGén es un sistema de valoración de riesgos en materia de violencia de género, una aplicación automatizada que solamente toma en cuenta la intervención o las declaraciones de la víctima, realiza una valoración de riesgos y le sugiere al juez que el nivel de riesgo es bajo, medio o alto. En los juzgados de guardia un nivel medio supone automáticamente una orden de alejamiento y prohibición de comunicación con la víctima, sea como sea y sin entrar en el fondo del asunto. Un riesgo alto supone una detención o prisión. Esto va a suponer que a partir de ahí hay un sesgo de confirmación por parte del juez que lo ve durante la investigación y del juez que sentencia ese asunto, porque va a tener que justificar que ese individuo ha estado en prisión y la prisión depende que se hayan dejado llevar del sesgo de correlación de la peligrosidad de los algoritmos.

Los algoritmos son secretos: no se conocen porque están protegidos por propiedad intelectual. En 2016 el Tribunal Supremo de Wisconsin evaluó un sistema de aplicación de algoritmos a la valoración criminal de riesgos en el caso Loomis. Y llegó a manifestar que los sistemas se pueden emplear cuando van en beneficio del reo, pero lo que es necesario es que la defensa pueda tener acceso a la lógica del algoritmo. Eso nos va a plantear serios problemas cuando estemos hablando, por ejemplo, de la lógica aplicada a las investigaciones en materia de seguridad nacional, de terrorismo, de atentados contra la ciberseguridad, contra infraestructuras críticas, etc. Actualmente los fiscales nos negamos a la aplicación de métodos intrusivos de investigación

(como por ejemplo troyanos) porque no podemos garantizar que sus códigos fuente sean materia clasificada. No se los demos a la defensa porque están en juego las formas de investigación del poder estatal. La publicidad de los algoritmos es lo que va a sustituir a la publicidad de los procesos. Los procesos van a ser aceptados por los sistemas expertos que vamos a autorizar pero vamos a tener derecho a conocer cómo funcionan los algoritmos porque así vamos a saber cómo vamos a juzgar.

Ahora mismo somos un caos y un maremágnum. La inteligencia artificial cambia todos nuestros papeles. ¿Qué va a hacer un fiscal? No necesitará acusar, bastará meterle los *í*tems al sistema para que se ponga en marcha. Puede que el futuro papel del fiscal sea garantizar que el procedimiento de valoración del algoritmo es correcto y que cumple las garantías del sistema. El juez reducirá su función y tendrá una realmente creativa en la segunda instancia. Los abogados van a tener que usar sistemas que realmente convenzan o pongan en evidencia las deficiencias de los algoritmos en el sentido de demostrar que no están pensados para un caso concreto. Y ahí es donde intervendrá la creatividad humana.

Esos son los riesgos que nos plantea la aplicación de la inteligencia artificial, y muchos más en materia de seguridad nacional. Skynet no está cerca pero tenemos que pensar muchas cosas antes de desplegar sistemas de inteligencia artificial con toda su intensidad en todo nuestro panorama social. Todavía el poder judicial humano es mejor de lo que nos queda por venir.

PANEL III

LA INVESTIGACIÓN EN LOS EJÉRCITOS ALIADOS. SOLUCIONES TECNOLÓGICAS PARA LOS NUEVOS ESCENARIOS

Au cont@ct. Un Ejército más ágil

Claude Chary

Coronel Responsable de Digitalización y de Coordinación de la Innovación en el Estado Mayor del Ejército de Tierra de Francia

La palabra innovación es un fenómeno de moda y el Ejército francés está haciendo un gran esfuerzo en términos de transformación digital e innovación para llevar a cabo mejoras. Esta innovación se debe a que nuestras fuerzas en operaciones, tanto en el Medio Oriente como en África, se enfrentan a organizaciones o grupos terroristas (como el Daesh) y a otros peligros que están explotando rápidamente tecnologías civiles duales. Cuando sufrimos ataques aéreos del Daesh con granadas mediante RPAS y solicitamos apoyo a nuestra agencia de construcción de equipos y materiales contra este tipo de amenaza no podemos aceptar que nos digan que nos harán un rifle antiaéreo en dieciocho meses. Por eso necesitamos acelerar la innovación. Y ese es uno de los ejes definidos en la orden de nuestro Jefe de Estado Mayor que se pondrá en marcha este año con la promulgación de la nueva Ley de Programación Financiera. A partir de ese momento la innovación en el ejército se basará en un sistema abierto que contará con la ayuda de los regimientos para acelerarla y diseñar nuevos sistemas, estableciéndose también procedimientos de experimentación.

La innovación es consustancial a los ejércitos y para nosotros es una cuestión de vida o muerte, por lo que debemos ser rápidos, acelerar el proceso de innovación y reducir los tiempos de desarrollo de dispositivos que posteriormente se puedan desplegar sobre el terreno. La innovación planificada está plagada de múltiples procesos relacionados con la industria, procesos que requieren mucho tiempo, son costosos y están vinculados a la transformación digital. Lo que queremos hacer es acelerar los estudios previos, proyectos RAPID[1], estudios técnicos operati-

1. Régimen de apoyo para la innovación dual para el descubrimiento de nuevas tecnologías.

vos, estimaciones tácticas y urgencias operativas. Todos ellos son administrados por la nuestra Dirección General de Armamento (DGA), conllevan largos periodo de tiempo y están llamados a reintroducirse en los programas de armas.

Para ello, queremos desarrollar e impulsar un sistema de innovación abierta. La innovación abierta consiste en, por ejemplo, facilitar medios económicos a un innovador que está destinado en un regimiento para que desarrolle sus ideas. Vamos a ayudar a los innovadores a implementar sus ideas y a experimentarlas gracias a una nueva Agencia de Innovación y Defensa (AID) creada a nivel Ministerio de Defensa y también vamos a ayudarles a escalar hacia la industrialización, pues aquí es donde generalmente mueren las innovaciones debido a su elevado coste. La AID está adscrita a nuestra DGA y establece medios para poner en contacto al ejército con la industria y con las universidades. También nos permite mejorar los procedimientos de contratación pública para ir más rápido. Nuestro objetivo es establecer un dispositivo que permita acelerar la innovación y tratar más fácilmente con la industria a todos los niveles. A este respecto, la DGA sigue siendo el primer interlocutor a nivel estatal, pero nuestras fuerzas también están autorizadas a interactuar e incluso a establecer protocolos con la industria a nivel local y también con las universidades.

Desde 2015 disponemos de una red de dispositivos básicos de innovación, como son los Puntos de Contacto Regimiento, y de estructuras tales como Célula de Datos y Célula Tecno-numérica. El pasado verano creamos la primera División de Organización Numérica y Coordinación de Innovación en el Estado Mayor para unir estos pequeños laboratorios y responder así a todas las peticiones de la DGA, cumpliendo de este modo con todo lo que se está estableciendo a nivel ministerial. En la División hemos creado una oficina que aglutina capacidades relacionadas con sistemas de información, seguridad informática, regulaciones europeas, regulaciones de protección de datos, etc. El nuevo equipo encargado de la transformación digital, compuesto por oficiales capacitados y con experiencia en análisis de datos (científicos de datos o investigadores operativos), trabaja en el ordenamiento de nuestros sistemas de datos para hacerlos crecer. Cabe decir que tenemos bien presente que la innovación no se limita solo a la transformación digital sino que también afecta a la doctrina, organización, recursos humanos y simplificación.

También se ha creado una unidad para transmitir la innovación. Para ello, en primer lugar hicimos un recorrido por todo el país para detectar las pequeñas cosas que obstaculizan la innovación, lo que nos permitió crear muchas herramientas para desbloquear procedimientos lentos y molestos. Además de estas herramientas disponemos de otras en internet y en nuestra red militar (*Intradef*) aplicadas a procedimientos de mayor envergadura. Todas ellas nos permiten equipar a nuestras unidades con soluciones móviles para que, entre otras cosas, puedan realizar trabajos de mantenimiento, que es donde estamos avanzando más. Estamos comenzando cinco proyectos de inteligencia artificial para el mantenimiento predictivo en relación directa con los recursos humanos, con el fin de disponer de oficiales que entiendan las necesidades, que sepan cómo diseñarlas y que puedan explicarlas a su cadena de mando. Un ejemplo de estos proyectos es el Proyecto EOTO[2] mediante el cual se evalúan conceptos, con o sin demostradores, para guiar los estudios de capacidades y la valoración de las amenazas.

Pero todo esto no puede funcionar si no se hace un esfuerzo en la gestión de los datos, que son el corazón del sistema. Por ello hicimos hincapié en mejorar las tecnologías con dos objetivos principales: reducir la carga en el régimen de entrada y mejorar su explotación por parte del personal de alto nivel. Gracias a ello disponemos de una política sobre datos, de una organización para almacenarlos y usarlos y comenzamos la transformación numérica.

En la actualidad estamos trabajando para cubrir toda la innovación, lo que implica recoger ideas desde la base de nuestra organización. Para ello hemos establecido una División Digital y Coordinación de la Innovación y hemos designado un representante para la innovación, la transformación digital y la simplificación en cada regimiento. A través de ellos, cualquiera que tenga una idea innovadora puede mostrarla, explicarla y posteriormente dirigirla directamente al Estado Mayor General del Ejército de Tierra. La alta gerencia puede dar su opinión pero no puede bloquearla. Cuando la idea llega a la División, todas las oficinas la estudian y la analizan para ver su grado de interés, su coherencia

2. Estudios operativos y técnico-operativos.

doctrinal, su viabilidad económica, etc. Cada dos meses se forma un comité directivo y se toma una decisión con respecto a su implementación. Esta es nuestra forma de plantear la innovación participativa y de acelerar los proyectos.

Este sistema también se emplea en un marco externo al ejército, porque la innovación abierta es participativa y dual. En consecuencia, tenemos proyectos abiertos con la industria y con las universidades. Por citar uno, el polo de desarrollo Innovación Tierra, en el que trabajan todas las grandes escuelas y universidades científicas y técnicas que están instaladas en París-Saclay, los principales sectores industriales franceses y nuestras principales direcciones militares, que son las encargadas de probar y de mantener los nuevos materiales y equipos. Este proyecto se desarrolla a nivel nacional pero también a nivel local. Existe un procedimiento que permite incorporar a estudiantes en prácticas para que puedan trabajar en un proyecto durante un año. Servimos de enlace para la celebración de contratos locales entre innovadores y desarrolladores y para la celebración de contratos con grupos de socios industriales regionales. Disponemos de un Centro de Innovación a nivel del Ejército y de la nueva Agencia Ministerial de Defensa de la Innovación, que puede firmar contratos con la industria y realizar estudios comparativos y experimentos a gran escala. Este dispositivo lleva en funcionamiento desde el 1 de julio de este año. Ya veremos si es eficiente.

Nuestras prioridades técnicas y operativas son la energía y nuevas energías, la protección de los soldados y la robótica. En todas ellas está presente la inteligencia artificial, por lo que debemos entrenar a todos nuestros militares para optimizar su empleo en cada nivel, lo que implica un esfuerzo añadido en términos de recursos humanos. Un jefe debe tener especialistas en inteligencia artificial a su disposición para asesorarse sobre lo que puede hacer y en qué confiar.

Otra característica de nuestra innovación es que es autónoma: en cuanto producimos un pequeño sistema lo ponemos en práctica. Tal es así que en el programa Scorpion (nuestro concepto de acción terrestre futura) se han ido introduciendo robots a medida que se iban produciendo, por lo que ahora nos vemos en la necesidad de tener que realizar estudios de innovación para reintroducirlos de manera acorde a las necesidades de desarrollo del programa. En consecuencia, vamos a experimentar con varios

de ellos primeramente en Francia y seguidamente en África. Este es un ejemplo sobre el cual la DGA considera que no se va lo suficientemente rápido y que está repercutiendo en la innovación abierta.

Mi papel en esta nueva división del Estado Mayor es hacer que las cosas sucedan. A principios del año pasado elevamos al Ministerio de Defensa una serie de propuestas precisas y cuantificadas para la transformación digital, con un presupuesto asociado de más de quince millones de euros por año. Tras las correspondientes negociaciones, el presupuesto recibió casi el 80% de financiación. Este año comenzamos de nuevo con la innovación, que evidentemente necesita recursos. Lo peor sería generar esperanza y decepcionar, por lo que tenemos cuidado de que lo digital no sea solo una cuestión de expertos. Tampoco debemos saturar a los jefes con una gran cantidad de datos sino hacerles llegar únicamente aquellos que les sirvan para obtener la información que necesitan en cada nivel de decisión.

Como no podía ser de otra manera, la innovación y la transformación digital, que es solo una parte de la innovación, son vitales para el ejército francés.

Soluciones del Ejército en investigación de materiales y experimentación

Mark Bailey

Coronel Jefe de la División de Experimentación del Centro de Conceptos y Desarrollo del Mando Futuro del Ejército de los Estados Unidos en el Estado Mayor del Ejército de Tierra de Francia

El ejército estadounidense está desarrollando un trabajo prospectivo de experimentación y modernización similar a la Fuerza 35 del Ejército de Tierra español para llegar a disponer de una fuerza con la que poder trabajar de manera conjunta con nuestros aliados en el futuro. Este trabajo se enfoca en tres áreas: modernización, experimentación e integración de la fuerza, que es nuestro verdadero desafío en todo lo que hacemos.

Existen muchas similitudes entre el ejército español y el de los Estados Unidos. Al igual que el español, nuestro ejército se está modernizando y transformando mediante un enfoque basado en capacidades. Nuestra intención es crear una fuerza que tenga la fortaleza suficiente para desplegar, combatir y vencer en cualquier campo de batalla en cualquier parte del mundo. Nuestros cronogramas de modernización también son muy similares. Nosotros estamos trabajando para poder disponer en 2028 de una fuerza capaz de operar en operaciones multidominio y de una fuerza preparada para intervenir en este tipo de operaciones en 2035. Por su parte, el ejército español está trabajando con unos plazos de tiempo similares con la intención de disponer de una fuerza modernizada en 2035 (la llamada Fuerza 35). Otra similitud radica en el modo en cómo vamos a afrontar la modernización, comenzando en primer lugar con un plan conceptual sobre cómo queremos combatir en el futuro, pasando a continuación a llevar a cabo una experimentación que permita validar conceptos y capacidades, para finalmente implementar lo validado mediante la compra de lo que se necesite para construir la fuerza que queremos.

Nuestro enfoque para llegar a alcanzar la modernización es similar al del ejército español. Primeramente procedemos a identificar las amenazas. En nuestro caso principalmente provienen

de Rusia y China, así que pensamos en conformar una fuerza que pueda competir con ellos en el campo de batalla con las fuerzas de estos países. Pero no podemos olvidar las amenazas provenientes de otros actores como Corea del Norte, Irán y organizaciones extremistas violentas como el Daesh. Una vez que una amenaza ha sido identificada procedemos a consultar los documentos Estrategia de Defensa Nacional y Estrategia Militar Nacional[1] para saber el modo en que la nación debe actuar ante una guerra futura y a partir ahí determinar cuál es el papel que debe desempeñar el ejército. Una vez conocido esto, nos centramos en cómo queremos llevar a cabo la guerra futura y esa idea se convierte en nuestro concepto.

Hace un año que nuestro ejército presentó el nuevo concepto de operaciones multidominio. Nuestra idea central es que debemos ser capaces de dirigir este tipo de operaciones para imponernos en la contienda y para poder penetrar y desintegrar los sistemas enemigos de negación aérea y antiacceso cuando sea necesario y así conseguir nuestros objetivos. Primeramente nuestro equipo de desarrolladores de conceptos procedió a definirlo, a continuación fue analizado en profundidad y después se desarrolló una estrategia de modernización con una indicación priorizada de los sistemas a modernizar y de hitos temporales que se deben cumplir para producir la fuerza necesaria.

De modo análogo al ejército español, el concepto de operaciones multidominio en el que se basa nuestra estrategia de modernización se analiza a través de la óptica de ocho elementos: doctrina, organización, preparación, materiales, formación, dimensionamiento, infraestructuras y políticas de implementación: debemos saber qué necesitamos cambiar en nuestra doctrina, qué necesitamos cambiar en nuestra organización, qué necesitamos cambiar en la forma en que dirigimos nuestra preparación, qué nuevos materiales o capacidades necesitamos, qué tipo de liderazgo y de educación necesitamos adoptar, si necesitamos aumentar el tamaño de nuestra fuerza o disminuirlo, qué tipo de instalaciones se requieren para mantener esa fuerza (áreas de entrenamiento, escuelas, etc.) y qué políticas deben cambiarse para implementar el concepto. Las respuestas a estas ocho preguntas

1. *National Defense Strategy* y *National Military Strategy*.

nos dirán básicamente cómo combatimos, con qué combatimos y quiénes somos. Si en la fase de experimentación se tienen en cuenta esos ocho elementos se podrá validar el concepto y comenzar con el desarrollo de la fuerza. De este modo podremos alcanzar en 2028 una fuerza capaz en operaciones multidominio y en 2035 una fuerza que esté preparada para combatir en este tipo de operaciones.

El proceso de experimentación comienza con la consideración de unos *inputs* y finaliza con la obtención de unos resultados, de manera análoga a otros ejércitos aliados. Los *inputs* son muy importantes y por ello estamos aprovechando fuentes de datos autorizadas para analizar y examinar de manera exhaustiva la amenaza con el objeto de determinar sus capacidades antes de elegir el ámbito geográfico en el que queremos realizar nuestros experimentos.

Consideramos el concepto de operaciones multidominio en su conjunto como el concepto operacional del ejército, pero para definir este concepto general también tenemos en cuenta los conceptos funcionales (que son las funciones de combate maniobra, fuegos, inteligencia, logística, etc). Analizamos cada uno de estos conceptos, nos hacemos las preguntas y buscamos sus respuestas para a continuación analizar las capacidades, tanto las nuestras como las de la amenaza en toda su amplitud (por ejemplo, para conocer cuál es el alcance de un sistema). Puede ser que algunas de las capacidades todavía ni existan, pero tenemos que saber con exactitud cuáles serán. Seguidamente consultamos los antecedentes de experimentos anteriores, incluidos los de menor entidad (tales como experimentos sobre determinadas capacidades o experimentos conceptuales). Y finalmente y lo más importante, nos centramos en determinar los objetivos de la experimentación, que básicamente son las preguntas a las que se quiere encontrar respuesta, cosa que parece fácil pero que realmente no lo es.

La experimentación se realiza mediante un proceso de planeamiento colaborativo multifuncional en el que desde un principio participa el máximo número de personas posible. Comenzamos con un proceso de deliberación que tiene como objetivo diseñar el experimento. Se introducen los objetivos de cada concepto funcional, es decir, tratamos de averiguar cuáles son las preguntas que una determinada función de combate debe responder. A continuación desarrollamos el escenario del experi-

mento. Si es Rusia, primero determinamos lo que creemos que va a hacer y después determinamos qué tipo de operación queremos hacer nosotros (ofensiva, defensiva u otra). Nosotros usamos todo tipo de experimentación: real, simulada, ejercicios, etc. Una cosa que nos gusta es hacer que nuestros soldados participen en los experimentos. Ellos conocen la doctrina actual y las capacidades actuales pero nosotros les pedimos que piensen en el futuro y en capacidades futuristas, lo que constituye un desafío porque a veces no entienden para qué están siendo entrenados. Finalmente, un grupo de analistas analiza los resultados del experimento para ver si realmente responden a las preguntas y si las soluciones obtenidas son aprovechables. La experimentación permite identificar mejoras e introducir cambios en los conceptos funcionales, tanto relacionados con materiales como con capacidades. De este modo estamos obteniendo los conceptos futuros.

Un desafío importante para nuestro ejército tiene que ver con la integración, algo que tenemos siempre presente y que es muy difícil de conseguir (es más fácil decirlo que hacerlo). Uno de los desafíos de integración surge al considerar las funciones de combate fuegos y logística. Sabemos que nuestras unidades de fuegos tienen un alto consumo de munición pero no sabemos cómo solucionar el problema logístico que ello genera (emplear más vehículos o tal vez vehículos más grandes). Otro desafío de integración consiste en hacer que la cadena de mando participe en los experimentos para facilitar la posterior toma de decisión en cuanto a la validez de las soluciones encontradas, lo que significa que debe aportar guías y orientación durante toda la planificación y ejecución de la experimentación. Con ello queremos asegurarnos de que quien tenga que tomar la decisión para desarrollar la fuerza futura disponga de la mejor información desde un principio.

Necesidad de cambio de los ejércitos actuales para afrontar las amenazas de la guerra híbrida

Neil Bellamy

Coronel Responsable del Área de Interoperabilidad de los Programas de Desarrollo para una Fuerza Futura de la Dirección de Capacidades del Cuartel General del Ejército del Reino Unido

La interoperabilidad es muy importante en nuestro día a día, tanto en el ámbito nacional como internacional. Independientemente de los problemas que identifiquemos, la solución pasa por la cooperación internacional, tanto a nivel político como a nivel militar. La amenaza cambia constantemente, pero el carácter del conflicto sigue siendo el mismo. En función de su intensidad llevamos a cabo una u otra acción conforme a esta escala creciente de actuación: proteger, comprometer, restringir, combatir. El extremo menos intenso de la escala es proteger, acción que se aplica tanto en territorio nacional como en cualquier territorio en el que estemos desplegados. El extremo opuesto se corresponde con el combate de alta intensidad derivado del artículo 5 de la OTAN. Si nos preparásemos únicamente para este tipo de conflicto estaríamos dedicando todo nuestro dinero y recursos a conseguir una capacidad de combate que nos permitiría actuar en una contienda que es poco probable que se produzca. En lugar de ello, tal vez debamos buscar equilibrar nuestros recursos para centrarnos en acciones de menor intensidad o incluso en acciones de combate en otro tipo de conflictos que es más probable que se produzcan.

Antes de nada nos preguntamos qué es la guerra. En la actualidad estamos lidiando con ataques químicos en territorio nacional, como por ejemplo el conocido incidente de Skripal en Salisbury. También lidiamos con ciberataques, tales como los que desprestigian a nuestros políticos a causa de las decisiones tomadas en relación con determinados conflictos. ¿Es así como se libra ahora la guerra? ¿Podemos proteger a nuestros políticos de esos ataques? Una segunda pregunta que nos hacemos es si no nos estaremos preparando para la última guerra. Si nos fijamos

en la flota de vehículos de nuestro ejército vemos que está pensada para combatir en grandes conflictos en el Medio Oriente y el sur de Asia, y eso no es lo que necesitamos en este momento. Una tercera pregunta que nos hacemos es si la guerra híbrida es la nueva forma que tenemos de guerra. A este respecto, resulta procedente sabe a qué llamamos guerra híbrida. ¿Tal vez a la zona gris de actividad o actividades bajo el umbral? Estamos ante un término que si bien a día de hoy es difícil de definir, sabemos que requiere una actuación conjunta basada en el equilibrio, la agilidad y la capacidad de respuesta.

Otro punto de importancia relevante es que, siendo conscientes de que nuestros adversarios evitarán enfrentarse a nuestros puntos fuertes y atacarán nuestras debilidades, no debemos continuar invirtiendo exclusivamente en nuestras fortalezas. Es necesario identificar todas las fortalezas y debilidades de nuestros adversarios y desarrollar nuestras capacidades en consecuencia. Algunos de nuestros adversarios (como Rusia) pueden estar en condiciones de desplegar rápidamente y podría ocurrir que cuando movilizásemos nuestras fuerzas de ventaja el conflicto ya hubiese finalizado. Así pues, debemos poder responder rápidamente y con agilidad para negarle así la ventaja posicional al adversario. Para ello necesitamos cambiar nuestra forma de pensar e impulsar las capacidades que se requieran.

El ejército del Reino Unido se configura en torno a tres áreas que requieren un equilibrio de esfuerzos: la capacidad de nuestro contingente, el compromiso en zonas de operaciones y la defensa del territorio nacional. Al desarrollar las tres áreas obtenemos nuestra agenda estratégica, que está caracterizada por la modernización, la maximización del talento, la eficacia del mando, la adaptación y eficiencia, la preparación y el dimensionamiento de los recursos humanos. Una de las características más importantes es la maximización del talento: si pretendemos lidiar de manera pragmática y rápida con cualquier situación que surja, debemos invertir en las personas y dotarlas de las herramientas adecuadas.

La definición del concepto operacional del ejército británico comienza con conocer las capacidades necesarias para actuar conforme requiera la intensidad del conflicto (proteger, comprometer, restringir, combatir). Debemos lograr un equilibrio explorando nuevas tecnologías y desarrollando nuevas capacidades. También debemos tener en cuenta una serie de principios clave

tales como nuevas capacidades de mando y control, mentalidad flexible y compromiso persistente, entre otros. Para ello debemos considerar los efectos que requiere el nuevo enfoque y desarrollar la habilidad necesaria para gestionarlos. A este respecto hemos conformado una sexta división que se ocupa de capacidades especiales, tal como la maniobra de información. Las divisiones primera y tercera se ocupan de la guerra convencional, pero no solo deben combatir en este tipo de guerra sino que deben hacerlo en todas las que puedan surgir en esta nueva era, y para ello deben disponer de un mando y control que sea capaz de gestionar capacidades que podrían no existir de manera uniforme. Por ejemplo, buscaremos reforzar la cadena de mando de división para que tenga capacidad de interactuar con departamentos del Gobierno, en otros entornos, con otras agencias y con socios internacionales. Finalmente, debemos explorar y usar la red global en las facetas humana, virtual y logística, toda vez que una nueva forma de operar requiere cambios culturales (lo que es tremendamente difícil de conseguir).

De todo lo que se debe tener en cuenta para definir el concepto operacional cabe destacar la necesidad de implicar a otros departamentos del Gobierno y a nuestros aliados. Necesitamos adquirir y explotar capacidades que nuestras divisiones no disponen en la actualidad. Y destacar también la 'velocidad de relevancia', que es importante para nosotros por dos razones: por nuestra intención de acelerar la adquisición de capacidades y de materiales del mañana y por la necesidad de obtener cuanto antes un enfoque que nos permita desarrollar capacidades para la fuerza actual, la fuerza futura y la fuerza conceptual. Quizás pueda ocurrir que capacidades que consideramos conceptuales y que no están disponibles estén siendo implementadas por nuestros adversarios. Conlleva bastante tiempo el que los ejércitos convencionales las introduzcan y las usen, por lo que la velocidad de relevancia es importante.

El problema clave para llegar a la fuerza futura que necesitamos es el reconocimiento, la modernización y la transformación. La forma en que tradicionalmente conseguimos la modernización es a través de programas de financiación, pero al ser muy costosos y requerir mucho tiempo estamos buscando la manera de transformar las capacidades y mejorarlas. Y lo hacemos mediante el uso de nuevas estrategias innovadoras tales como el capitalismo

de riesgo, la innovación de defensa y la optimización de la colaboración con la industria de defensa y con la universidad. Pero no podemos alcanzar este costoso *hard power* sin el equilibrio necesario en una amplia gama de capacidades y de efectos (nucleares, convencionales y subliminales).

En todas las zonas de operaciones en las que estamos desplegados debemos mantener nuestro compromiso de impedir el acceso a determinados recursos por parte de nuestros adversarios, de intercambiar el desarrollo de capacidades con nuestros aliados y de competir fuera de las áreas principales de conflicto. No solo debemos combatir con nuestros socios en los mares del sur de China o en las regiones bálticas. En muchos aspectos, nuestros adversarios (Rusia y China) ya no están gastando energía en áreas que nosotros consideramos clave y en las que esperamos su actuación sino que están explotando oportunidades en otras partes del globo, como por ejemplo en América del Sur o Central y en África, lo que nos obliga a estar en condiciones de competir con ellos en cualquier parte del mundo.

El Reino Unido está haciendo un esfuerzo para alinear conceptos, amenazas, recursos y políticas. Primero hemos desarrollado una serie de capacidades de forma independiente para después conjuntarlas de manera equilibrada y conseguir así capacidades combinadas de fuegos tempranos, refuerzo, capacidad de respuesta y capacidades reales, por ejemplo. Los soldados deben ser el corazón de cualquier capacidad. Los sistemas robóticos autónomos aumentan la eficiencia, pero nunca podrán reemplazar la necesaria intervención humana en la toma de decisiones (a este respecto existe un dilema ético y los países lo enfocan de diferentes maneras). Consideramos que el entrenamiento es muy importante: las nuevas tecnologías permiten adiestrar a la fuerza para que pueda actuar en cualquier parte del mundo en una guerra tipo, en la cual se incluiría el entrenamiento en las capacidades necesarias para abordar nuestras debilidades en la zona gris, tales como técnicas de distracción, nuevas barreras y vigilancia continua que conecte sensores con tiradores de modo que se puedan realizar ataques en profundidad. La guerra tipo nos permite capacitar a los soldados para que experimenten en primera línea y se adapten rápidamente a los cambios. Hay muchas iniciativas innovadoras relacionadas con la experimentación en la guerra tipo, pero la más destacada es la de guerra autóno-

ma. El pasado año experimentamos 71 dispositivos robóticos y autónomos en todo tipo de servicios, para lo que contamos con la participación de 47 socios industriales. Esta colaboración ha tenido una inversión conjunta de cinco millones de libras por parte del ejército y de diez millones de libras por parte de la industria. Trabajando conjuntamente conseguimos una mayor eficiencia, superando así el tiempo en el que la industria no contaba con nuestros requisitos (lo que suponía una importante pérdida de recursos económicos), y gracias a ello se han identificado una serie de plataformas que ahora estamos desarrollando. Habida cuenta del éxito obtenido, este mismo procedimiento será el que usemos cuando encaremos la iniciativa de la guerra autónoma en marzo del próximo año.

Por último, he de mencionar la importancia del capital humano. Desarrollamos un programa (denominado Programme Castle)[1] en el que se designó a una persona para que se encargase específicamente de que hiciéramos lo que hiciéramos para transformar el Ejército no dejáramos a nuestra gente atrás. Con respecto a este capital humano nos preguntamos cuál es la futura estructura profesional que se requiere, qué preparación y formación se requiere y qué sistema de gestión basado en el talento se necesita para llevarlo a cabo. La realidad es que el cambio es difícil y la velocidad de transformación no coincide con la variación de la naturaleza de los conflictos. Así que debemos trabajar más duro, equilibrar la modernización y la transformación, mantener el equilibrio entre los aliados, los socios y el panorama político y ser más asequibles, porque si no lo somos no obtendremos apoyo. Finalmente, debemos guiarnos con visión y conceptos coordinados, porque aunque sean sutilmente diferentes, los conceptos no dejan de ser los mismos.

1. Programa Castillo.

Enfoque del Ejército de Tierra ante los retos de la transformación

Julio Salom Herrera
General de Brigada Jefe de la División de Operaciones del Estado Mayor del Ejército de Tierra

Con respecto a los escenarios futuros en los que vamos a operar debemos preguntarnos cuál es el diagnóstico principal: qué tenemos que hacer y dónde vamos a tener que operar, y desde ahí conocer nuestras necesidades y carencias y cuál será es el elemento clave al que dirigirnos en este nuevo ciclo.

Para ayudar a resolver estas preguntas la División de Operaciones del Ejército de Tierra dispone de la Sección de Ayuda a la Decisión, en la que existe un Observatorio compuesto por sociólogos, investigadores operativos, estadísticos y una serie de oficiales muy capaces que informan de manera continua sobre cómo estamos operando fuera, cuál es la moral de combate de las unidades y si éstas están bien diseñadas. Somos un Ejército cuya razón de ser se basa en la creación de estructuras operativas, por lo que una de nuestras misiones principales es la de evaluarlas y corregir errores.

Estamos moviéndonos en un entorno complejo, inestable, incierto y que está marcado por una omnipresencia de la información, que caracteriza la gestión del cambio en el que nos encontramos. Sabemos que vamos a desenvolvernos en entornos muy cambiantes y caóticos en los que la rapidez de la decisión es algo transversal. Las situaciones inestables van a aparecer en cualquier momento, cualquier comandante y en cualquier entorno va a estar saturado de información (no de inteligencia), lo que condicionará permanentemente el planeamiento de las operaciones. Si antiguamente el reto de cualquier jefe era saber lo que había detrás de la colina, hoy en día sabemos tanto de lo que hay detrás que el reto es conocer la situación, despejar el ruido para conocer la melodía.

Es por ello que la gestión de la información y del conocimiento será uno de los retos más importantes a los que nos vamos a enfrentar, y para encararlo nos tendremos que apoyar en los procesos de gestión: la inteligencia artificial. En ese aspecto tenemos que ver siempre qué es lo que nos dice el jefe y qué es lo que quiere. Nuestro Jefe del Estado Mayor del Ejército nos ha dicho que quiere dirigir al Ejército a un entorno del año 2035, que quiere mirar al futuro y que quiere un ejército equipado con las mejores tecnologías, pero teniendo a la vez preparado y motivado a su personal para que sea la herramienta realmente resolutiva en el combate. De una parte preliminar, en la que el MADOC tuvo un protagonismo esencial al decirnos hacia dónde íbamos a ir y cómo íbamos a combatir, se pasó a otra en la que se creó un entorno de experimentación dentro de una brigada (concretamente la Brigada Rey Alfonso XIII de la Legión). Esta brigada permitirá meter en un banco de pruebas los nuevos conocimientos y los nuevos materiales que están llegando a través de la industria de defensa para ver si somos capaces de integrarlos y de adaptar a ellos nuestra organización y nuestros procedimientos.

En el futuro escenario nos moveremos en una zona gris: no vamos a saber si estamos en conflicto, la crisis será permanente, actuaremos en un espacio de batalla no lineal, las unidades van a estar muy aisladas, posiblemente en un entorno de áreas urbanizadas, combatiremos con presencia de población civil y tendremos siempre previsto que podremos enfrentarnos a un enemigo altamente tecnificado o equivalente en capacidades a nosotros. Con esa serie de parámetros tenemos que ir diseñando nuestras unidades. Siempre tendremos en cuenta el carácter masivo de la información (por lo que tendremos que dosificarla para evitar saturar a los escalones intermedios y bajos) y la necesidad de compartir en detrimento de la necesidad de conocer. Es decir, inteligencia basada en saber administrar la información, puesto que de no ser así se podrían colapsar los cuarteles generales de brigada y los puestos de mando de batallón y compañía.

El problema con el que nos vamos a encontrar proviene de la resistencia al cambio y a abandonar la zona de confort. Es necesario vencer ese miedo y aliarse con las tecnologías. Tenemos que buscar situaciones de ventaja en el combate, para lo que debemos hacer uso de las nuevas tecnologías y ser capaces de ir viendo realmente cuáles nos sirven y cuáles nos saturan.

Es la brigada donde el Jefe del Ejército ha decidido que se integren todos los nuevos materiales y los sistemas de experimentación, porque es el sistema de combate integral que se ha dado al Ejército como eje principal de diseño. Vamos a mirar cómo afecta la tecnología a nuestros procedimientos de combate desde el enfoque del estudio del MIRADO[1], pero en esta ocasión lo vamos a hacer al revés, vamos a hablar del DOMIRA: primero empezaremos por el estudio de la doctrina y la organización, ya que es importante que antes de nada veamos cómo van a ser nuestros procedimientos de combate y cómo vamos a organizarnos, y después procederemos a integrar los materiales y a ver las infraestructuras y los recursos que hay que asignarles. No nos cabe duda de que tenemos que ir a estructuras más pequeñas, más potentes y más eficaces que puedan actuar más aisladas en el combate. Por eso necesitamos un sistema de mando y control robusto que tenga capacidad para que la información fluya y que aporte un sistema de referencia en el que todos los ejércitos aliados y todas las funciones de combate puedan estar presentes en el mismo escenario. No seremos interoperables si un sensor ofrece las coordenadas de un objetivo y resulta que las unidades no tienen el mismo plano referenciado. Esa es la primera base: tener un mapa referencial del que todos podamos beber, que la información pueda fluir, que los sensores puedan ir integrando esa información desde todos los niveles y que el comandante pueda ver exactamente qué es lo que está pasando.

Para eso tenemos en marcha un simulador constructivo en el Centro de Adiestramiento de San Gregorio, gracias al MADOC y a la JCISAT. Ya estamos estudiando la integración de simuladores para que tengamos todas las funcionalidades de combate integradas en un único simulador desde nivel división hasta nivel compañía, porque no cabe duda de que todos los sensores van a estar alimentando el combate de una forma excesivamente profusa. Nuestro sistema de inteligencia tiene una gran dificultad para integrar todo el conocimiento. Somos conscientes de que las nuevas tecnologías aportan mucha información y que son además una gran oportunidad. La inteligencia de fuentes abiertas es po-

1. Material, Infraestructura, Recursos humanos, Adiestramiento, Doctrina y Organización.

siblemente una de las principales fuentes de información en los sistemas de inteligencia actuales, pues todo el mundo tiene una necesidad imperiosa de contar todo lo que hace. Simplemente siendo capaces de discernir y de ver que está haciendo el adversario podemos tener el acceso a muchas fuentes. Otras fuentes de información a considerar son las procedentes de la inteligencia de señales, de la inteligencia electrónica y de fuentes humanas, la cual es insustituible.

Necesitamos que nuestros medios y fuerzas sean modulares, porque vamos a estar trabajando en coalición. Tendremos que beber mucho de los sistemas no tripulados, de la automatización y de una conducción remota, porque esto nos va a ahorrar bajas y nos va a permitir combatir con fuerzas aliadas.

La fuerza de maniobra en superficie, que será esencial para las fuerzas terrestres, debe garantizar la protección del combatiente, debe disponer de unos fuegos muy precisos y profundos que permitan tener que llevar menos carga de munición pero a la vez influir más directamente en el combate, y debe ser capaz de combatir tanto montada como desmontada, es decir, de interactuar en el combate en un ataque de gran intensidad pero relacionándose con la población.

En cuanto a la logística, vamos a necesitar unos especialistas que se enfoquen más en el diagnóstico que en la reparación, una construcción aditiva que permita disminuir los *stock* y unos sistemas que aprovechen la energía solar o eólica para disponer de puestos de mando que tengan una menor huella logística y mucha menos firma térmica y electromagnética (gracias a sistemas como los que ya está experimentando la Universidad Politécnica de Madrid con unidades de nuestro Ejército, por ejemplo).

También tendremos que orientar la preparación para que nuestro combatiente sea mucho más polivalente. El combatiente debe ser una persona capaz de manejar los últimos materiales pero capaz también de interactuar en otros escenarios. Es decir, un soldado de artillería no podrá estar enfocado solo a disparar con su cañón sino que tendrá que tener también conocimiento de control de masas y de zonas y tendrá que estar preparado para combatir en cualquier situación de manera análoga a un soldado de infantería.

Nosotros hemos hecho un esfuerzo para definir e identificar el problema y ahora tenemos que pedir a la Universidad y a la

Empresa que nos ayuden a investigar para disponer de una respuesta tecnológica a nuestras necesidades. Hasta ahora el binomio Universidad – Empresa ha funcionado muy bien y en España lleva más de treinta años trabajando con grandes desarrollos. Nosotros queremos dejar de ser unos meros aprovechadores de oportunidades para ser un vértice del triángulo Universidad–Empresa–Ejército. Tenemos que decirle a la Universidad cuáles son nuestros problemas, la Universidad tiene que ayudarnos a hacer un desarrollo conceptual y la Empresa debe ser capaz de transformar los conceptos en nuevos materiales. Nosotros los probaremos y les daremos un nuevo valor añadido, puesto que cuanto mejor probados estén más rendimiento sacará la Empresa. Un ejemplo de esto es el trabajo que se está llevando a cabo en colaboración con las Universidades de Granada y Jaén, que constituye un modelo a imitar y a exportar al resto de los ámbitos del conocimiento en España. A este respecto, la Secretaria de Estado de Universidades e I+D+i pronunció la siguiente frase: «Aspiramos a una adecuada colaboración entre investigadores y empresas para que la investigación científica se traduzca en aplicaciones técnicas e industriales».

Queremos que el elemento humano entienda perfectamente cuál es la misión y sepa exactamente cómo generar confianza y un entorno de aceptación en cada una de las operaciones en las que se participe. En la actualidad tenemos unidades desplegadas en cuatro ámbitos en los principales escenarios: una brigada en el Líbano como fuerza de interposición, donde nuestras tropas están mezcladas con la población civil de distintos componentes étnicos y religiosos; una fuerza importante en Iraq, donde estamos circunscritos a una base militar en la que solo interactuamos con soldados iraquíes; una fuerza de entrenamiento en Koulikoró y Bamako (Malí), que está trabajando con el ejército pero interactuando con la población; y una fuerza en Letonia participando en una importante operación de disuasión en la que se interactúa con población civil y ejércitos aliados. En el Ejército de Tierra tenemos claro, como principio, el respeto y la confianza en el mando que se encuentra sobre el terreno. Tendremos mucha información, pero ninguna podrá sustituir a la proporcionada por elemento humano sobre el terreno (por eso la opinión del comandante que se encuentra desplegado será siempre un elemento fundamental). También sabemos que por mucha información que

tengamos de nuestros contactos y por muy exhaustivo que sea nuestro planeamiento, no hay plan que resista la primera hora de combate, sobre todo si nos enfrentamos a un enemigo tecnológicamente avanzado que va a saber cuáles son nuestras carencias y que va a saber esperar y atacar nuestras debilidades. De ahí la importancia de que nuestros hombres sean capaces de aprovecharse de la tecnología y de saber «replegarse» a situaciones de ambiente degradado. Podremos quedarnos sin posicionadores y sin sistemas de mando y control pero tendremos que ser capaces de volver a un sistema de trabajo cercano al tradicional.

En el Ejército de Tierra también estamos afrontando el tema de la preparación, porque no hay sistemas tecnológicamente avanzados que sean útiles si el combatiente no es capaz de usarlos. Por eso estamos trabajando en un plan piloto que permita a nuestros hombres acelerar la adquisición de un talento digital. Si tradicionalmente el Ejército ha sido una vía de socialización de nuestros soldados (en los años sesenta y setenta a través de la alfabetización y educación y en los años ochenta y noventa a través de cursos de formación profesional), hoy en día tenemos que conseguir que vuelvan a la sociedad siendo expertos en talento digital. El programa piloto se está implantando en tres niveles: a nivel sénior, para que nuestros mandos sean conscientes de la innovación digital; a nivel medio, para que los mandos intermedios sean capaces de conocer las nuevas aplicaciones; y a nivel tropa, para que nuestros soldados conozcan las nuevas tecnologías.

Otro reto asociado al que nos enfrentamos está relacionado con la ética de los conflictos. Debemos ser conscientes de que la inteligencia artificial nunca va a relegar la responsabilidad del comandante a la hora de tomar decisiones, por lo que tendremos que modular también nuestros planes de estudios para que nuestros oficiales y suboficiales egresen con ese tipo de formación.

PANEL IV

TECNOLOGÍA Y NUEVOS MATERIALES: ROBÓTICA, DRONES, NANOTECNOLOGÍA Y REALIDAD AUMENTADA

Necesidades tecnológicas del Ejército de Tierra

Fernando García y García de las Hijas
General de División Jefe de la Dirección de Adquisiciones del Mando de Apoyo Logístico del Ejército de Tierra

En el marco de la seguridad y de la defensa de los intereses de España, para la Fuerza Terrestre es muy importante estar en la vanguardia tecnológica mediante la participación imprescindible y activa de las industrias y de las universidades. Esta interacción entre el mundo del conocimiento y de la investigación que aporta la Universidad, junto con la Industria y con el Ejército es lo que garantiza realmente que haya una defensa fuerte. España sigue claramente el ejemplo de los países de nuestro entorno, contando con la Industria y con los organismos de investigación como aliados para conseguir un objetivo común: la defensa de España y de su soberanía.

Los dos ejes en los que articulamos las necesidades tecnológicas son la Fuerza 35 (que es la visión del Ejército de Tierra como motor de la innovación) y el Proyecto Tecnológico de la Base Logística del Ejército de Tierra, apoyado decididamente por el Ministerio de Defensa y que ya es una realidad.

En cuanto a este primer eje, la captura de la innovación en la Fuerza Terrestre se hace a través de un instrumento que se llama Foro 2E+I (Ejército – Empresa e Innovación – Investigación), que comenzamos en mayo de 2018 y que hemos revalidado en octubre de este año. Es un modelo abierto, directo y continuado de confluencia entre los requerimientos operativos del Ejército de Tierra y las posibilidades tecnológicas que aportan la investigación, el desarrollo y la innovación a través de las industrias y de las universidades. El foco es la Fuerza 35: modelo, visión y solución del Ejército de Tierra al planeamiento de la defensa y motor de la innovación que apunta a situarnos en la vanguardia tecnológica en 2035, si hacemos los deberes desde ahora.

Perseguimos una alianza de confluencias e intereses en ese «triángulo de oro» que conforman el Ejército (de la mano de la

Dirección General de Armamento y Material–DGAM, particularmente de la Subdirección General de Planificación, Tecnología e Innovación-SDG PLATIN), las empresas y las universidades. Buscamos decididamente la integración colaborativa como horizonte inmediato, pero teniendo bien presente que la situación final deseada es cambiar el paradigma de obtención para poder dotarnos de una forma más eficiente y más eficaz con el objeto de reforzar la capacidad operativa y la potencia de combate de la fuerza terrestre.

El camino es complejo, pero ilusionante. Sin duda tenemos importantes retos en I+D, como identificar las necesidades y posibilidades a futuro y establecer las líneas de investigación y mantener el trabajo de forma adaptativa y continuada. Por eso, antes y después de cada Foro, mantenemos la llama de la interacción, confluencia y mutualidad de intereses en una serie de talleres específicos sobre determinadas capacidades de combate que nos van a abrir oportunidades de experimentación y de investigación, soportados por una interacción colaborativa que consideramos fundamental.

En cuanto a los retos de adquisición de ahora a 2035, es fundamental la coordinación entre la estructura del consumidor (la Fuerza Terrestre), los potenciales proveedores y la Universidad. La situación final deseada es disponer de un nuevo modelo de adquisición global (NOCET)[1], completo, equilibrado e interoperable con el foco puesto en la brigada como unidad de referencia y como sistema de combate conjunto, completo e integral, tal y como recoge el Objetivo de Capacidades Militares del Jefe de Estado Mayor de la Defensa. Sin olvidar además, la coherencia y compatibilidad de los sistemas de armas en la adquisición a corto, medio y, sobre todo, a largo plazo, teniendo en cuenta los ciclos de obsolescencia y la velocidad e incertidumbre en el cambio.

El impulso tecnológico en la Fuerza 35 queda jalonado a través de una serie de avances tecnológicos. En primer lugar debemos tomar en consideración la capacidad autónoma y sistemas robóticos. Ya la estamos valorando en vehículos no tripulados, en

1. Nuevo sistema de Obtención de Capacidades del Ejército de Tierra. Consiste en implantar un modelo cíclico de obtención horizontal de brigadas completas en base a las capacidades de combate.

especial en sistemas UAS[2] y UGV[3]. Los UAS deberán poder reaccionar frente amenazas y llegar a detectar y evitar posibles zonas hostiles en vuelo. Se prevé la evolución de los sistemas de navegación para el vuelo en zonas de GPS denegado. En UGV se deberá evolucionar a una completa capacidad a nivel de convoyes, partiendo de la capacidad autónoma a nivel de vehículos individuales (que está ya en el estado del arte). Otra tecnología importante a tener en cuenta es la derivada de la inteligencia artificial. En este ámbito los avances irán enfocados al apoyo en la toma de decisiones y a la mejora de los tiempos de respuesta desde la detección a la neutralización de amenazas. La inteligencia artificial también permitirá mejorar el grado de filtrado de la masificación de datos captados por innumerables sensores. Y otro avance tecnológico es el proporcionado por el Control Común[4], que tiene capacidad de fusionar la información en tiempo real facilitando así la interoperabilidad. Se requieren nuevas capacidades en las redes C4I[5] y se deberá trabajar en red. Toma mayor relevancia el combate colaborativo. Es importante no solo fusionar la información sino también minimizar los tiempos en la parte de la conciencia situacional (observar y orientar) para dedicar más tiempo a la toma de decisiones y disponer de más tiempo para dar respuesta y actuar frente a la amenaza.

La capacidad RAS[6] es fundamental para la fuerza terrestre. El horizonte RAS para las proximas décadas está caracterizado por la proliferación de sensores portátiles, combatientes ampliamente sensorizados, transporte autonomo, creciente uso de vehículos no tripulados, sistemas de limpieza de rutas, sistemas de desactivación de explosivos, municiones autónomas y automatizadas, vehículos ISTAR[7] y vehículos de combate no tripulados. Por funciones de combate, en inteligencia perseguimos el uso de sensores avanzados enfocados a la adquisición inmediata de información;

2. UAS: sistema aéreo no tripulado (*Unmanned Aerial System*).

3. UGV: vehículo terrestre no tripulado (*Unmanned Ground Vehicle*).

4. Pack de software único para controlar todo el despliegue de sistemas terrestres y aéreos.

5. Mando y Control, Comunicaciones, Computación e Inteligencia.

6. Sistemas autónomos y robóticos *(Robotic and Antonomous Systems*).

7. Inteligencia, vigilancia, adquisición de objetivos y reconocimiento (*Intelligence, Surveillance, Target Acquisition and Reconnaissance*).

en apoyo logístico buscamos la robotización de vehículos en primera instancia, el desarrollo de vehículos totalmente autónomos, el transporte en la última milla en zona de combate, transportes logísticos, convoyes autónomos y capacidad de autodiagnóstico de nuestros sistemas de armas; en protección es fundamental la capacidad contra IED[8] de manera totalmente autónoma y la detección de la amenaza NBQ; en maniobra y fuegos, por mencionar algunas, las unidades mixtas de sistemas tripulados y no tripulados, el uso de armamento en sistemas RAS (tipo munición *loiter*[9]*)* y el uso de máquinas de ingenieros autónomas.

Los resultados buscados desde el punto de vista del impulso tecnológico de la Fuerza 35 se perfilan a través de tres procesos interactivos: la fase conceptual, con la definición de conceptos (en la que el MADOC tiene un peso específico fundamental); la fase de experimentación, que se hace a caballo de nuestra plataforma de experimentación (la BRIEX, que es la Brigada de la Legión en Almería), cuya valoración se vuelve a hacer por el MADOC; y la fase de implementación, que incluye no solamente los proyectos de obtención sino los proyectos de I+D que incorporamos a través de los programas de I+D de la Dirección General de Armamento y Material. Estos tres procesos se repiten en la fase inicial para alcanzar la fuerza posible (actual ciclo de planeamiento), en el siguiente ciclo de planeamiento con una programación y con una interacción mucho más integrada para alcanzar la fuerza avanzada y finalmente para conseguir la fuerza de ventaja, objetivo final de nuestra vanguardia tecnológica. A corto plazo nuestro esfuerzo se centra en experimentar en la BRIEX y la adquisición de sistemas inmediatos (el estado del arte) con la ayuda de SDG PLATIN. A medio plazo es importante orientar los proyectos tecnológicos de I+D del Ministerio de Defensa a través de innovaciones tecnológicas para futuros programas que también lleva la Dirección General de Armamento. Y finalmente, el horizonte por descubrir y que tenemos que hacer de la mano de la investigación son los desarrollos tecnológicos de I+D+i para la fuerza de ventaja.

Como hemos mencionado, el Foro es un instrumento continuado, abierto y directo, que se articula en grandes plenarios anuales y

8. Artefacto Explosivo Improvisado *(Improvised Explosive Device).*
9. Munición merodeadora (*Loitering Ammunition*).

se complementan con talleres específicos. El próximo tratará sobre sistemas contra RPAS. Los resultados de estos talleres se articulan en tres grandes áreas: conceptos derivados para la Brigada 2035, oportunidades de experimentación en la BRIEX y propuestas de I+D para influir e inspirar la política de I+D del Ministerio de Defensa; destacar, por ejemplo, los programas de UGV como propuesta de I+D, láseres pulsados, fotónica, el empleo de la luz, etc.

Si el primer eje para articular nuestras necesidades tecnológicas es la Fuerza 35, el segundo es el Proyecto Tecnológico de la Base Logística del Ejército de Tierra. Supone una apuesta decidida por una modernización e incremento de la eficiencia en toda la cadena logística del Ejército de Tierra. Supondrá la inversión en infraestructura más importante en lo que va de siglo. El Ministerio de Defensa contempla realizar una inversión de trescientos millones de euros en unas instalaciones en las que van a poder trabajar más de mil cuatrocientas personas. Consiste no solo en concentrar los actuales centros logísticos (tenemos doce en la actualidad) sino en centrarnos en el gran componente tecnológico, esto es, aplicar y desarrollar lo que conocemos como Industria 4.0 y denominamos Logística 4.0, inteligencia artificial, IoT, *big data*, nanotecnologías, 5G, tecnologías cuánticas, etc.

La Base Logística tiene un gran componente tecnológico que ya está en desarrollo y que permite optimizar y agilizar los procesos logísticos. En la actualidad ya se están realizando prototipos y demostradores con distintas universidades sobre robotización, impresión 3D, simulación y mantenimiento predictivo. El General de Brigada Rafael Tejada, Jefe de la Ingeniería del Mando de Apoyo Logístico del Ejército de Tierra (JIMALE), en colaboración con determinadas universidades, está procesando los distintos demostradores y prototipos que van a ayudar a hacer el diseño tecnológico de esta realidad.

Con la Fuerza 35 y con el Proyecto Tecnológico de la Base Logística el Ejército de Tierra apuesta decididamente por una anticipación disruptiva. El valor incremental de la experimentación, de la demostración y de la investigación permitirá maximizar sistemas y tecnologías disruptivas e incrementar exponencialmente la ventaja operativa. La Fuerza 35 no solamente es un cambio de entorno operativo, un cambio de organización frente a la misión y un cambio de sistemas de materiales sino también un cambio de cultura y mentalidad hacia la cultura de la urgencia.

Para concluir, hacemos nuestras las palabras enunciadas por el Secretario de Estado de Defensa, en la clausura del segundo Foro 2E+I, (con más de ochenta empresas y diecinueve universidades presentes): «Reconocimiento para todas aquellas personas que se dedican o que destinan una parte muy importante de su tiempo a pensar en el futuro, dando muestras de una gran generosidad y de una gran inteligencia. Generosidad porque están haciendo un trabajo desinteresado cuyos frutos recibirán otros e inteligencia porque está claro que se recoge lo que se siembra. Tenemos necesidad de planear con anticipación y habrá que recibir aquello que se planifica, aquello que se siembra. Las Fuerzas Armadas no pueden cumplir su misión sin una industria fuerte. Y la industria española no puede avanzar sino es con el apoyo del Ministerio de Defensa. Todos juntos, con el talento que nos aporta la universidad y que España tiene, y en abundancia, es lo que va a permitir que España sea un país cada vez más fuerte, unas Fuerzas Armadas y un Ejército de Tierra cada vez más moderno y que todos podamos cumplir esta noble y gran misión que es defender a nuestro país, defender España, defender la paz y defender la libertad».

Capacidades de las empresas españolas

Manuel de Oliveira Astray
Vicepresidente Ejecutivo de la División de Defensa de Everis Aeroespacial Defensa y Seguridad

Las capacidades de las empresas españolas son muy amplias, pero más allá de entrar en el detalle acerca de ellas debemos situarnos en el momento en el que está la industria española y en cuáles son los retos a los que de alguna manera se enfrenta.

Everis Aeroespacial Defensa y Seguridad es una división del grupo Everis, el cual trabaja focalizado en el mundo de la seguridad, aeronáutica, espacio, defensa y simulación. Tiene un modelo que lleva operando desde hace diez años basado en la inversión en pequeñas y medianas empresas nacionales que tienen un producto y una tecnología diferencial en el mundo de la defensa, con la idea de buscar las sinergias entre esa tecnología diferencial y las capacidades de comercialización, internacionalización y financieras que tiene una gran compañía como es Everis. Este modelo nos ha permitido trabajar en el desarrollo de drones, sistemas autónomos aéreos, sistemas de armas (como el porta-mortero Alakran, usado en el Ejército de Tierra y creado por NTGS), reconocimiento facial, simulación aérea, simulación terrestre, cámaras embarcadas en satélites de órbita baja que permiten una gran definición, tecnología fotónica, etc.

Según los datos de TEDAE[1], el sector de la defensa en España supone aproximadamente el 1% del PIB nacional y el 6,1% del PIB industrial y emplea cerca de cincuenta y siete mil profesionales de forma directa en un trabajo de alta calidad y con un alto componente de innovación. El porcentaje de exportación que tiene la industria nacional de defensa, seguridad y aeronáutica es de un 66%. Cuando se exporta se consigue que una parte impor-

1. Asociación Española (de empresas) de Tecnologías de Defensa, Seguridad, Aeronáutica y Espacio.

tante de la autonomía estratégica que proporciona la industria de defensa a las Fuerzas Armadas la paguen países aliados a los que se vende material por autorización del Gobierno, influyendo al mismo tiempo en su autonomía estratégica.

La industria de defensa en España se encuentra en una encrucijada provocada por la orientación que la Unión Europea está tomando en relación con la industria y política de defensa. Europa ha decidido dejar de dar la espalda a la defensa e invertir decididamente en el desarrollo de capacidades que garanticen la autonomía en este ámbito. El EDF es un buen ejemplo de inversión para promocionar la investigación y el desarrollo de dichas capacidades de una manera decidida con un modelo de competencia colaborativa.

Comparando la inversión europea en defensa con la de los Estados Unidos, la inversión por soldado en Europa es de un poco más de un cuarto de lo que invierte el país norteamericano. En cambio, donde los estadounidenses tienen treinta sistemas de armas en Europa tenemos ciento setenta y ocho, donde tienen un sistema acorazado nosotros tenemos diecisiete, donde tienen cuatro destructores o fragatas en Europa hay veintinueve y donde tienen seis aviones de combate nosotros tenemos veinte.

El que haya un fondo de defensa invirtiendo en proyectos y desarrollos conjuntos y la comparativa con los Estados Unidos en cuanto a inversión en defensa se refiere nos lleva a una conclusión evidente: en Europa tiene que haber una concentración de capacidades alrededor de la industria. Lo que quiere Europa, y lo que necesita, es concentrar esas capacidades en otras más claras. Sun Tzu, en su libro titulado El arte de la guerra, dice lo siguiente: «La configuración del terreno puede ser un apoyo para el ejército. Para los jefes militares, el curso de la acción adecuada es calibrar al adversario para asegurar la victoria y calcular los riesgos y las distancias. Salen vencedores los que libran batallas conociendo estos elementos. Salen derrotados los que luchan ignorándolos». Quiero decir con esto que debemos conocer nuestra competencia y conocer el entorno para identificar cuáles son las capacidades reales que tenemos.

Hoy en día las cosas han cambiado para tener liderazgo tecnológico en un área determinada. El 31 de enero de 1958 se lanzó desde los Estados Unidos el primer satélite que orbita la Tierra (el Explore 1, también conocido como Alpha 1). Por entonces,

el liderazgo tecnológico en un área estaba al alcance de pocas naciones. Pero en la actualidad internet ha democratizado la innovación. Valga como ejemplo el caso de Julián Fernández, un joven español de dieciséis años, quien junto a dos jóvenes británicos y uno checo ha diseñado un pequeño satélite de doscientos cincuenta gramos de peso y cinco centímetros de lado que se va a poner en órbita el próximo 25 de noviembre para dar cobertura a la IoT.

España tiene capacidades tecnológicas en determinadas áreas que hoy en día son líderes en el mundo, tales como capacidades robóticas de desactivación de explosivos, capacidades en inteligencia de video, capacidades en reconocimiento facial (una compañía española, Herta, *spin off* de la Universidad de Barcelona, compite en el mundo en cuanto a reconocimiento facial no colaborativo) o capacidades en tecnología UAV[2] (por ejemplo, la compañía nacional SCR con su RPAS Atlantic, con un UAV operacional y con la compañía DAS Photonic).

La pregunta que surge es saber si pueden las compañías nacionales llegar a competir con otras compañías de Alemania, Francia o Italia, por ejemplo. España tiene un presupuesto de defensa que es aproximadamente la mitad del italiano, un tercio del británico y cerca de una cuarta parte del francés. Para que nuestra industria pueda competir con la de otros países y garantizar que desempeñamos un papel importante tiene que jugar en la clave del liderazgo tecnológico en nichos clave. España tiene hoy compañías pequeñas y medianas que ostentan liderazgo tecnológico gracias a la democratización de la innovación. Para poder competir con otros países necesitamos algo que ya nos está proporcionando el Ejército de Tierra con la Fuerza 35. Los ingenieros de defensa siempre decimos que el acceso al operativo es el bien más escaso de la industria de defensa. Los ingenieros tenemos que conocer el problema real que hay que resolver y no el que nosotros nos imaginamos en nuestros despachos. La Fuerza 35 nos está permitiendo trabajar con los operativos e identificar estos problemas.

2. Vehículo aéreo no tripulado *(Unmanned Aerial Vehicle)*. También conocido como RPAS o dron, pero el uso de UAV suele ir frecuentemente referido drones de uso militar.

Un ejemplo de experiencia de éxito que tiene que ver con la industria española y con el acceso al operativo es el URO VAMTAC[3]. El programa nació en 1998 cuando el ejército español decidió dar el desarrollo a la compañía gallega UROVESA. En su primera versión no era el mejor que había en el mercado, pero hoy en día y después de un esfuerzo de especificación y de refinamiento por parte del Ejército y de un esfuerzo por aprender por parte de la industria, el VAMTAC es un vehículo muy competitivo. Si Europa decidiese agregar o congregar los vehículos tácticos ligeros y la industria española tuviera que competir en ese campo, seguramente URO tendría mucho que decir. Otro ejemplo es el Pizarro[4], un desarrollo de la industria española que hace Santa Bárbara General Dynamics en colaboración con la industria austriaca que ha permitido a esta empresa ser la adjudicataria del desarrollo del vehículo británico equivalente y ser la única empresa europea que compite para fabricar el vehículo equivalente para el ejército de los Estados Unidos. Además, otra empresa española (SAPA) ha desarrollado un grupo de motor transmisión de vehículos pesados que ha sido elegido por el gobierno estadounidense para equipar sus vehículos de menos de cincuenta toneladas. Ambas compañías españolas son dos ejemplos de empresas que trabajando en tecnologías concretas y focalizadas en un nicho tecnológico están siendo capaces de competir en el mundo.

Por su parte, Everis tiene un UAV operacional que se ha desarrollado gracias a un programa de la Dirección General de Armamento y Material. Nuestro UAV no tiene nada que envidiar a ningún otro europeo y podría competir perfectamente con algunos de los mejores del mundo. Quizás en el estado del arte esté Israel, pero desde el punto de vista operativo hay pocas capacidades que tengan los israelitas que no tengamos ya, y si seguimos invirtiendo a buen seguro que adquiriremos una calidad diferencial. Esto es autonomía estratégica.

Cabe mencionar a la compañía DAS Photonics, *spin-off* de la Universidad Politécnica de Valencia, que tiene una tecnología para la conversión de señal de radiofrecuencias a señal óptica que permite que su procesamiento sea mucho más rápido en todo el

3. Vehículo de Alta Movilidad Táctica.
4. Vehículo blindado de combate.

espectro radioeléctrico, ofreciendo unas capacidades hasta ahora no conocidas en la guerra electrónica y en la radárica, por ejemplo. Cabe decir que para el ejército estadounidense esta tecnología española está hoy por encima de cualquier otra en el mundo.

Como conclusión, la industria de defensa española tiene suficiente capacidad para competir en un nuevo entorno europeo que va a imponer un sistema de competencia – colaboración. Potenciando tecnologías y desarrollos en nichos concretos seguiremos en el liderazgo tecnológico en Europa. Desde el punto de vista de Everis, esa es la manera en la que vamos a garantizar que somos exitosos.

Capacidades y proyectos de investigación de la Universidad de Granada

Francisco Gámiz Pérez

Responsable del Laboratorio Singular de Nanoelectrónica, Grafeno y Materiales Bidimensionales de la Universidad de Granada

La Universidad es el templo del conocimiento y como tal nuestra misión y obligación es la de generar conocimiento a través de la investigación. Pero también es nuestra obligación transferir ese conocimiento para formar nuevos profesionales y transferirlo también al sistema productivo y al empresarial de nuestra sociedad. Dentro de poco más de diez años la Universidad de Granada será una institución cinco veces centenaria. Y lejos de ser una institución arcaica y obsoleta se reinventa cada día tratando de dar soluciones a una serie de problemas que nos demanda la sociedad para una vida más inteligente en diferentes dominios. En el dominio de la salud y el bienestar se están desarrollando sistemas económicos de diagnóstico precoz de enfermedades, como por ejemplo el proyecto Five Minutes and Fifty Cents que se está llevando a cabo en el Parque Tecnológico de la Salud junto a grupos de investigación de esta Universidad con la idea de diagnosticar enfermedades como el cáncer en un tiempo muy corto y con muy poco dinero. También son importantes las soluciones en el transporte y la movilidad (como por ejemplo, el desarrollo de vehículos autónomos), en defensa, en sistemas de energía y medio ambiente (como por ejemplo, el desarrollo de fuentes de energía alternativa no contaminantes), en el ámbito de la comunicación y en el *infotainment*[1] (como por ejemplo, añadir nuevas prestaciones a los equipos que permitan recortar el tiempo de salida al mercado y reducir costes). Dar soluciones para una vida más inteligente en estos dominios es el desafío más grande que tiene nuestra sociedad y nuestra Universidad en los próximos años.

1. Información y entretenimiento (*Information and Entertaiment*).

Una herramienta para conseguir una vida más inteligente es la nanoelectrónica. Hace quince o veinte años mejorar un nodo tecnológico significaba aumentar el poder de computación de los sistemas y aumentar el poder de almacenamiento de información de los sistemas (es lo que hoy en día usa masivamente Google en su granja de datos en Oregón, por ejemplo). Pero eso ya no es suficiente hoy en día. Hoy lo que necesitamos y buscamos es que ese poder de almacenamiento y de cálculo sea móvil y esté disponible en todo lo que nos rodea: en nuestro *smartphone*, en nuestra *tablet*, en nuestro vehículo, en el frigorífico de la casa, etc. Es lo que se viene a llamar el dominio More Moore. Gordon Moore, uno de los fundadores de Intel, predijo en 1965 que el número de dispositivos que se van a incluir en un circuito integrado se duplicaría cada dieciocho meses. Cuando aparecen los primeros microprocesadores en el año 1970, incorporan aproximadamente dos mil trescientos transistores. Hoy en día los microprocesadores incorporan más de mil trescientos millones. Pero eso no es el milagro Moore. El milagro Moore es que todos esos transistores se introducen en el mismo espacio en el que hace cincuenta años se metían solamente dos mil trescientos, lo que ha sido posible gracias a la miniaturización de los dispositivos. Pero eso ya no es suficiente hoy en día. Estos sistemas nos permiten tener un cerebro muy rápido y prodigioso y ejecutar avanzados algoritmos de inteligencia artificial. Pero estos algoritmos no funcionarán si no tienen datos que procesar, y las decisiones que toman estos algoritmos no sirven para nada sino se ejecutan. Los sistemas necesitan estar embebidos en el entorno, tomar información del ambiente y poder ejecutarse posteriormente. Todo esto es lo que llamamos el dominio More than Moore. Y para que la solución sea más inteligente se necesita que todo se haga a bajo coste económico. IoT será un éxito si conseguimos que todos los sensores y sistemas que tenemos que desarrollar y extender no sólo tengan un bajo coste económico sino que además sean baratos energéticamente. Y si además la energía se puede obtener de manera autónoma del medio ambiente y del entorno que les rodea, obtenemos lo que para nosotros es una solución para una vida más inteligente.

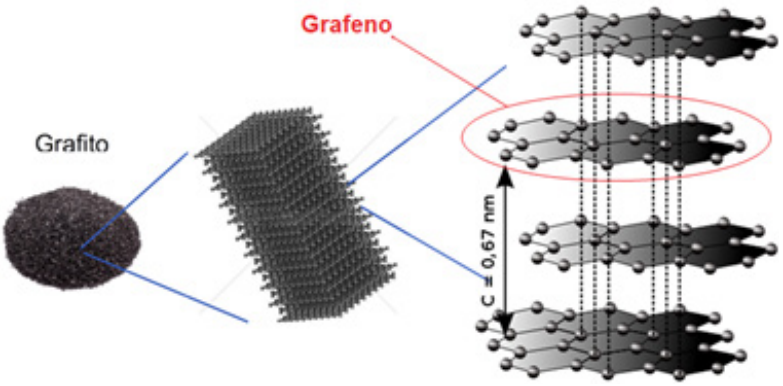
En resumen, las soluciones que se están buscando, para las cuales se está trabajando y generando conocimiento en la universidad, necesitan mayores prestaciones, es decir, necesitan de la

combinación de los dominios *More Moore* y *More than Moore,* además a bajo coste energético y a bajo coste económico. Y para eso es importante la miniaturización de los dispositivos (el escalado de los dispositivos).

Pero nuevamente hoy en día eso no es suficiente, ya que se necesitan nuevas estructuras, nuevos materiales y se deben afrontar nuevos desafíos. Esto no significa que estemos llegando al fin de la época del silicio y de la electrónica tal y como la conocemos. El silicio vino para quedarse, pero vamos a tener que combinarlo con otros materiales, con otras tecnologías y encarar otros desafíos. La Universidad de Granada ha apostado por ello y ha invertido en el desarrollo de un Centro de Investigación TIC y en el de diferentes laboratorios singulares, en particular en el Laboratorio de Nanoelectrónica, Grafeno y Materiales Bidimensionales o en el reciente Laboratorio 5G. Estos laboratorios incorporan una serie de equipamientos únicos en España que nos permiten caracterizar dispositivos electrónicos de última generación, desarrollar materiales bidimensionales al mismo nivel que los mejores centros tecnológicos de todo el mundo y fabricar dispositivos electrónicos que después vamos a emplear en diferentes aplicaciones. Gracias a esta tecnología, a esta infraestructura y a la inversión se han podido implementar en el último año una serie de líneas de investigación básicas que, por ejemplo, nos han permitido desarrollar «la celda de memoria más pequeña jamás fabricada» precisamente cincuenta años después de su invención por Robert Dennard en IBM, lo que constituyó noticia de la agencia Europa Press. Este es el resultado de un proyecto europeo que estamos coordinando desde la Universidad de Granada (Proyecto REMINDER) y para el que se ha utilizado un material que no es silicio (en este caso, arseniuro de galio e indio).

Otro material que nos sirve para mejorar las prestaciones del silicio es el grafeno. El grafeno es un material compuesto por carbono puro que se distribuye o se organiza en una red plana hexagonal con un átomo de carbono en cada uno de los vértices de cada hexágono (los profesores de la Universidad de Mánchester Andre Geim y Konstantín Novoselov recibieron el Premio Nobel de Física en 2010 por haber aislado por vez primera en un laboratorio una monocapa de grafeno en el año 2004). El carbono aparece en la naturaleza en forma de diferentes alótropos. Químicamente el diamante y el grafito son exactamente el mismo

material, carbono puro, pero las propiedades estructurales son completamente distintas. El diamante es el material más duro que existe en la corteza terrestre, mientras que el grafito es un material que se exfolia (lo usamos, por ejemplo, en la punta de los lápices, porque al aplicar una presión sobre él se descompone en láminas y deja un trazo). La única diferencia entre estos materiales estriba en la manera en que se disponen los átomos tridimensionalmente: en el caso del diamante los átomos establecen fuertes enlaces covalentes en todas la direcciones del espacio, mientras que en el caso del grafito los átomos establecen enlaces fuertes únicamente en un plano formando capas que se unen entre sí mediante fuerzas mucho más ligeras y suaves (las fuerzas de Van der Waals). El grafeno es cada una de las capas o planos que conforman el grafito. Esta disposición atómica le confiere unas propiedades espectaculares, tanto mecánicas como ópticas, eléctricas (es el mejor conductor eléctrico que existe en la corteza terrestre conocido por el hombre), es muy buen conductor térmico e incluso impermeable.



Estructura atómica del grafito

En la Universidad de Granada podemos obtener grafeno mediante diferentes procedimientos, tanto a partir de la exfoliación mecánica y química del grafito como a partir de la descomposición del metano a altas temperaturas. Con ese grafeno desarrollamos diferentes aplicaciones, como por ejemplo electrodos transparentes (hoy en día se hacen con ITO, dióxido de estaño e indio, que es un material muy caro y rígido, y que podemos encontrar

en las pantallas de los móviles), circuitos flexibles y transparentes, *displays* electroforéticos flexibles, supercondensadores, baterías portátiles y sensores (de temperatura, de gases, de deformación mecánica o incluso biológicos). Podemos fabricar circuitos sobre una hoja de papel o sobre cualquier tipo de tela, tejido o material flexible. Por ejemplo, combinando un electrodo transparente flexible y un electrodo eléctrico flexible hemos desarrollado un *display* electroforético flexible, de manera que podemos pasar de un formato rígido como un *e-book* (rígido) a uno flexible como un periódico electrónico. Aplicando diferencia de tensión podemos cambiar el color de un *display* para pasar de un gris oscuro a un gris mucho más claro, lo que aplicado en tela se podría usar para el camuflaje, por ejemplo. Podemos desarrollar baterías portátiles flexibles que sirven para alimentar e iluminar un diodo led. Podemos crear diferentes tipos de sensores que ya podíamos hacer con silicio. Pero el grafeno permite poder bajar su umbral de detección a niveles mucho más pequeños: en el caso del silicio se pueden detectar concentraciones micromolares y nanomolares pero cuando incorporamos materiales bidimensionales jugamos con concentraciones picomolares, femtomolares e incluso atomolares (lo que permite detectar amoniaco o explosivos en muy bajas concentraciones, por ejemplo).

Además del grafeno hay una serie de proyectos que se desarrollan en esta Universidad en colaboración con Defensa, como son los Proyectos de Investigación del Centro Mixto UGR-MADOC (CEMIX) que durante los años 2014 y 2018 han permitido desarrollar más de veintiocho proyectos en diferentes disciplinas (tecnología, estrategia, legislación, salud del combatiente, seguridad, inteligencia artificial, etc.). También hay proyectos más ambiciosos, como los proyectos del Programa COINCIDENTE del Ministerio de Defensa e incluso proyectos financiados por la Unión Europea, cuyos objetivos tienen una clara aplicación en el campo de la defensa.

Un proyecto que se desarrolló con el CEMIX ha sido el de un radar ligero UWB[2] que se puede incorporar en dispositivos UAV y permite detectar, por ejemplo, la frecuencia cardíaca y el movimiento de la caja torácica, por lo que se ha aplicado para

2. *Ultra Wide Band:* banda ultra ancha.

la detección de presencia humana a través de un obstáculo. Un ejemplo de proyecto europeo es el SEMBA-UGR FDTD, desarrollado por un consorcio liderado por la Universidad de Granada en el que participan otras universidades y otras empresas españolas, el cual desarrolla un simulador basado en diferencias finitas en el dominio del tiempo para el estudio y resolución de problemas de compatibilidades electromagnéticas de modo que, por ejemplo, se pueda hacer el cálculo de la radiación de una antena colocada en dispositivos móviles. Dentro del Programa COINCIENTE se ha desarrollado el proyecto INDOTAC, consistente en la construcción de un dispositivo UAV para trabajos en entornos interiores (este dispositivo está desarrollado íntegramente con tecnología desarrollada en la Universidad de Granada).

Hoy en día nuestra sociedad está basada cada vez más en la tecnología. Somos tecnológicamente dependientes. Estamos desarrollando aplicaciones de alto nivel que necesitan una infraestructura (*hardware*) para poder ejecutarse. Si uno mira la lista de empresas fabricantes de dispositivos semiconductores en el mundo verá que en el primer cuatrimestre de 2019 no hay ninguna empresa europea en el *top* 10. Nos estamos disputando el liderazgo tecnológico con China y con los Estados Unidos y no tenemos fabricantes que puedan proporcionar a nuestras empresas dispositivos para poder implantar la red 5G, por ejemplo (que será la base para desarrollar la inteligencia artificial). Pero lo preocupante no es que no haya ninguna empresa europea en ese *top* 10 sino que la suma de la cuota de mercado de las empresas del *top* 10 suma el 99%.

	Company	Revenues 1Q18*	Revenues 1Q19	Market share	Revenue Growth	Country
1	TSMC	8547	7028	48.1%	-17,8%	Taiwan
2	Samsung	3253	2785	19,1%	-14.4%	Korea
3	GlobalFoundries	1513	1234	8,4%	-18.4%	USA
4	UMC	1292	1058	7,2%	-18.1%	Taiwan
5	SMIC	831	654	4.5%	-21.3%	China
6	Tower Semiconductor	313	310	2.1%	-0.9%	Israel
7	Powerchip Semiconductor	341	251	1.7%	-26.4%	Taiwan
8	VIS	221	225	1.5%	1.6%	Taiwan
9	Hua Hong Semiconductor	210	220	1.5%	4,7%	China
10	Dongbu HiTek	131	132	0.9%	1.1%	Korea

*Million USD Source:TrendForce

Top 10 de empresas fabricantes de dispositivos semiconductores en 2019

En octubre de 1973, después de la guerra del Yom Kipur, los países árabes miembros de la OPEP liderados por Arabia Saudí declararon un embargo de petróleo a los países europeos. Eso provocó la primera gran crisis energética (el precio del barril de petróleo pasó de tres dólares a más de quince). Personalmente no tengo claro que hayamos aprendido alguna lección de aquello. Hace escasamente tres meses Japón y Corea del Sur se han enzarzado en una guerra que aparentemente no tiene mucha explicación. Japón restringe las exportaciones a Corea del Sur de tres productos que no son leche, agua o pan sino poliamida, fotoresina y fluoruro de hidrógeno, precisamente los materiales que emplea la industria tecnológica de Corea. La respuesta del gobierno coreano ha sido crear un programa de investigación nacional dotado con diez mil millones de dólares a desarrollar entre 2020 y 2022 para tratar de reducir la dependencia tecnológica de Japón y del exterior (por cierto, la Universidad de Granada está presente en esa convocatoria de proyectos).

Con todo lo expuesto he intentado proporcionar unos ejemplos del conocimiento generado en la Universidad de Granada que ponemos a disposición del Ejército y de las empresas por si interesa y puede ser útil para el desarrollo de la Fuerza 35.

Ciberseguridad en dispositivos

José Antonio Álvarez Bermejo
Profesor Titular de Universidad en Arquitectura y Tecnología de Computadores del Departamento de Informática de la Universidad de Almería

La ciberseguridad es un campo extenso que relaciona un gran número de áreas y de disciplinas. Para introducir el escenario en el que nos movemos en el campo de la seguridad en sistemas podemos partir de un ejemplo comparativo. Imaginemos la casa de Gran Hermano: la casa en sí es el *hardware* (el procesador) que proporciona los recursos que están a disposición de los concursantes, que en este ejemplo se corresponden con el *software,* es decir, los procesos o programas en ejecución; los recursos disponibles van a ser compartidos por personas que potencialmente generarán conflicto, pero además nuestro procesador ejecuta programas que tampoco son los mejores ejemplos de programas y por lo tanto está asegurado el conflicto; existe otro *software* especial escondido que se encarga de instaurar la seguridad y el orden en ese procesador (el sistema operativo, que en nuestro ejemplo es el Súper o persona que controla la interacción entre las personas de la casa); y además hay otro *software* (el *firmware* o BIOS[1]) que es el responsable de introducir al Súper en la casa antes de que entren las demás personas. La BIOS, por tanto, gestiona y controla los recursos (casa) y al sistema operativo (Súper).

Si tratamos de atacar el sistema en este escenario a vemos que no solo el software es vulnerable sino que también es posible violar la seguridad del *hardware*, la seguridad del *software*, la seguridad del *sistema operativo* y la seguridad del *firmware*. Siguiendo con el ejemplo, las personas (programas) pueden interactuar entre ellas (o exclusivamente con la casa) afectando a la disponibilidad de recursos comunes e incluso llegando a abusar de recursos de otras

1. Sistema básico de encendido y apagado *(Basic Input Output System*).

personas (es decir, acceder a los recursos en memoria de otros programas); pero, afortunadamente, el Súper (el sistema operativo) lo impedirá. Esto era así hasta que se desveló la existencia de vulnerabilidades como Spectre[2] y Meltdown[3]. A partir de entonces cualquier persona (programa en ejecución o proceso) puede acceder a los recursos compartidos de cualquier otra y además se pueden habilitar mecanismos para anular al Súper y que éste no intervenga para restaurar el orden, provocando una situación inmanejable. La vulnerabilidad afecta a todos los sistemas basados en Intel desde 1995 hasta la fecha. Precisamente Intel acaba de anunciar su reciente avance en la arquitectura Intel Tiger Lake[4] que presenta protección ante esta vulnerabilidad (informada públicamente en 2018). Como cuestión abierta se plantea si esta vulnerabilidad se conocía antes y si se había aprovechado con anterioridad.

Se emplea mucho esfuerzo y recursos para garantizar la seguridad del software e incluso del hardware. Pero se invierte muy poco esfuerzo en securizar el firmware. Aún con todo, la industria civil –que es la que más ha ignorado hasta ahora la necesidad de revisar las cuestiones relacionadas con la seguridad– todavía no implementa las medidas necesarias. Por ejemplo, cuando un desarrollador realiza una implementación y esta implica el uso de librerías, ¿cómo asegurar que la librería que está siendo usada no incorpora vulnerabilidades? O peor aún, ¿cómo saber que la librería usada no incorpora ya funciones maliciosas que abren puertas traseras en el sistema que ejecuta el programa que las usa?

En la actualidad ya se distribuyen librerías que incluyen informes de auditorías de seguridad. Es cierto que una librería segura el día de hoy puede dejar de ser segura en unas pocas horas, pero al menos ofrece la garantía de que en su desarrollo incorpora medidas contra las vulnerabilidades más conocidas. Téngase en cuenta cómo operan quienes pretenden atacar a los sistemas: se documentan sobre las últimas vulnerabilidades conocidas de

2. Referencia: Moritz Lipp et al. Meltdown: Reading Kernel Memory from User Space. 27th USENIX Security Symposium (USENIX Security 18).

3. Referencia: Paul Kocher et al. Spectre Attacks: Exploiting Speculative Execution. 40th IEEE Symposium on Security and Privacy (S&P'19).

4. Referencia: Intel Tiger Lake. https://en.wikipedia.org/wiki/Tiger_Lake_(microarchitecture)

las librerías más usadas y dedican su tiempo a buscar programas desarrollados con estas librerías. El ataque es, como se puede fácilmente imaginar, inminente y de esperar.

Seguidamente se plantean una serie de cuestiones abiertas a modo de reflexión: si el software -que es fácil de actualizar y de distribuir- presenta estas vulnerabilidades, ¿a qué vulnerabilidades nos someten el *hardware* y el *firmware* de los dispositivos que usamos en nuestra esfera personal? ¿Y en la esfera laboral? ¿Y en la industria? ¿Y en los vehículos -civiles o militares- que manejamos? ¿Somos capaces de escalar la dimensión de la superficie de ataque que exponemos cuando usamos tecnología extranjera?

Como ejemplo para poner en contexto la importancia de todo esto se puede citar el gravísimo error que cometió un estudiante de doctorado al modificar la librería OpenSSL (https://www.openssl.org/), una de las más importantes en la conexión segura de un cliente con un servidor, la cual proporciona una capa de cifrado de extremo a extremo proporcionando así confiabilidad en la comunicación con un servidor (como por ejemplo en el caso https://mail.google.com/mail/u/0/#inbox), modificación que permitió usar la librería de manera maliciosa[5]. (Figura 3).

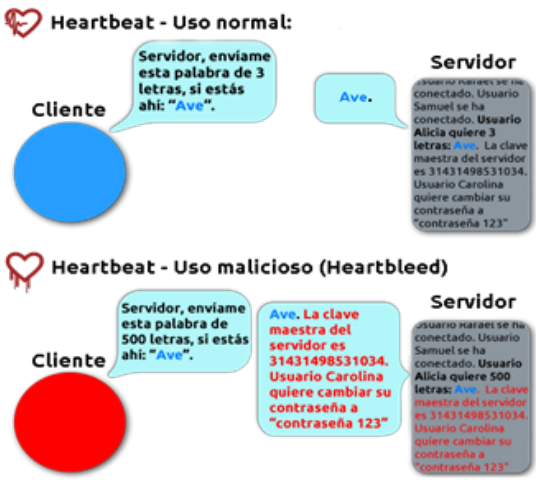


Figura 3. Vulnerabilidad introducida en OpenSSL

5. La noticia se puede encontrar en https://www.independent.co.uk/life-style/gadgets-and-tech/news/coder-responsible-for-catastrophic-heartbleed-bug-says-it-can-be-explained-pretty-easily-9254053.html

Esto debe hacernos reflexionar: aunque el equipo de ingenieros que desarrolle una aplicación para un entorno industrial, militar o civil sea excelente, es probable que cometa el error de utilizar librerías en sus desarrollos que no estén debidamente construidas, o que estando debidamente certificadas sean actualizadas sin cuidado, generando vulnerabilidades como en el referido.

Igual que el software convencional incorpora librerías desarrolladas por terceros (con intereses o no contra la seguridad nacional), los dispositivos *hardware* se construyen utilizando componentes diversos, muchos de los cuales portan su propio *firmware* (imposible de revisar por quien lo va a usar). En el caso de China, principal potencia mundial en el desarrollo de componentes hardware, este *hardware* lo desarrollan empresas que pertenecen al gobierno.

En relación con la dimensión de la amenaza, el hecho de que la ciberseguridad sea un tema que se trate en revistas y foros especializados en armamento ya deja entrever la dimensión del problema al que nos enfrentamos. Por poner un ejemplo, en la revista *European Security&Defence* 03/19 podemos encontrar un artículo denominado *5G and Battlespace Dominance* en el que se habla de la importancia del 5G y de cómo quien lidere esa tecnología liderará el campo de batalla. En él se concluye que la estrecha relación entre el gobierno de China y las empresas chinas más destacadas a nivel mundial que son líderes en el desarrollo de tecnología y *hardware* para sistemas de telecomunicaciones supone un potencial vector de penetraciones dirigidas en las cadenas de suministro de componentes microelectrónicos utilizados en los entornos militar, civil (Administración) e industrial de alto valor, como son la industria de defensa y de telecomunicaciones. Es decir, China fabrica componentes y desarrolla el *firmware* que éstos incorporan, por lo que pueden crear puertas traseras en cualquier dispositivo que deseen.

La respuesta a la pregunta de cómo puede llegar ese *firmware* a dominar todo un sistema computacional es sencilla: al iniciar un equipo, este no dispone de sistema operativo y debe «cargarlo» desde un sistema de almacenamiento. Esta labor la realiza la BIOS (el *firmware* principal del sistema), para lo que primeramente de debe revisar todo el *hardware* (componentes como tarjetas de red, etc) que están conectadas a él y tomar como parte suya el *firmware* de cada dispositivo. Es decir, cuando se inicia el proceso de arranque la BIOS revisa cada tarjeta conectada al sistema, y si esta tarjeta trae su propio programa (*firmware*) éste se copia junto

al *firmware* principal. Cuando termina este proceso el *firmware* del sistema se compone de todo el *firmware* contenido en cada dispositivo *hardware* conectado. Por lo tanto, si nuestro sistema operativo está preparado para solventar una vulnerabilidad concreta (como la protección NX) es posible que el *firmware* la desactive antes de cargar el sistema operativo.

A tenor de lo expuesto, cabe hacerse las siguientes preguntas: ¿dependemos de tecnología extranjera en sectores estratégicos tales como la defensa? ¿Es segura? ¿Pueden desactivar y activar a voluntad componentes en vehículos estratégicos?

Mi labor investigadora en la Universidad de Almería se centra en la implementación de técnicas criptográficas seguras diseñadas por investigadores de mi grupo de investigación «Categorías, computación y teoría de anillos» (FQM-211), entre los que se encuentra el doctor Juan Antonio López Ramos. Nuestro trabajo lo realizamos en colaboración con el grupo de investigación DITEC de la Universidad de Granada. Nuestra experiencia trabajando en la computación móvil, dispositivos empotrados y sensores con criptografía de curva elíptica nos ha enseñado que la bondad de cualquier criptosistema depende del sistema y de la pericia de quien lo implementa. Aún así, todo se termina desarrollando sobre componentes de terceros que son imposibles de controlar. Es extraordinariamente necesario que nuestro país aproveche el potencial investigador de sus universidades para no depender de componentes críticos desarrollados por potencias extranjeras.

Aunque la criptografía sea imbatible en el marco teórico, al poner el sistema a trabajar en determinado *hardware* aparecen problemas que permiten que otros entren en él y roben el núcleo del criptosistema haciéndolo totalmente inservible. Por tanto, hay que plantearse cómo de expuestos estamos ante las puertas traseras que nos pueden abrir y cuál es la posibilidad de vulnerar un nodo de una red de sensores, por ejemplo. Se deben incorporar términos como *rootkits* y *bootkits* en nuestro haber.

Así pues, el componente *software* (*firmware*) que coloca el sistema operativo, es decir, la persona que coloca a quien tiene que instrumentar la seguridad en la Casa de Gran Hermano, tiene la clave de todo el sistema. Esa persona es el *firmware* o BIOS. ¿Quién proporciona a esa persona? El *hardware*. ¿Y quién es el mayor manufacturador de *hardware* del mundo? China. Por lo tanto, al no ser seguro el *firmware* aparecen nuevas vulnerabilidades en

el subsistema de entrada y salida que permiten diseñar puertas traseras de acceso a nuestros sistemas. Cada vez que se enciende el ordenador se inicia un proceso de pre-arranque en el que se hace un acopio de información del sistema. Acto seguido se llama a la BIOS para que entre y empiece a cargar el sistema operativo. Si el pre-arranque y la BIOS no los controlamos, es posible que el *firmware* haya sido cuidadosamente manipulado para interferir en la interrupción (0x13) y para emular la interrupción 19 (que es la que se encarga de cargar el sistema operativo en memoria) de modo que nuestra nueva interrupción 19, a la par que lee el contenido del sistema operativo que va a copiar en memoria, puede realizar modificaciones sobre él, tales como modificar el sistema para que acepte cualquier contraseña como válida, cargar un módulo sin firmar, etc. Si este *firmware* se emplaza en dispositivos comerciales ampliamente usados es posible infectar a millones de sistemas. Si trasladamos esto a nuestro socorrido ejemplo de la casa de Gran Hermano, significa que la persona (con muchos privilegios) de Gran Hermano que coloca al Súper (al sistema operativo) dentro de la casa para que controle la interacción entre los concursantes, es capaz de adquirir su voluntad haciendo uso de ingeniería social. A partir de este momento el sistema tiene abierta una puerta trasera interesante. El Súper se convierte en un ser corrupto a merced de las órdenes de una persona externa, que le enviará peticiones a través de la persona que le dio acceso a la casa. El Súper podrá exigir comportamientos y acciones abusivas a los concursantes y considerar que son legales.

¿Qué pasa si además ese sistema se prepara para la descarga de un *bootkit* o de una herramienta que permite atacar un sistema? Pues que tenemos un sistema latente esperando a que desde cualquier punto de internet se entre en él por la puerta que se ha abierto en la BIOS. ¿Y dónde actúan los antivirus y las detecciones de intrusos? Actúan a nivel de sistema operativo pero no actúan a nivel de *hardware*. Entonces pensaríamos en reiniciar la BIOS y actualizarla, pero ¿qué ocurriría si el *firmware* malicioso viniese insertado en el chip de la tarjeta de red? En este punto es donde surge la pugna y se revela la batalla que hay entre China y los Estados Unidos. Robert Spalding, General de Brigada de la Fuerza Aérea de los Estados Unidos, pronunció la siguiente frase: «Cuanto más conectados estemos, y el 5G es la tecnología que más conectividad nos va a dar, más vulnerables seremos». China quiere

introducir su *hardware* y *firmware* y quiere dominar el espacio de 5G. Dominar el pre-arranque es clave, ya que al dominarlo se es capaz de modificar el núcleo de un sistema operativo para violar, por ejemplo, la protección de 'no ejecutar' o para actuar sobre él.

No es extraordinariamente difícil desarrollar una puerta trasera en el *hardware* de un ordenador. Sólo hacen falta cuatro condiciones: hacer que sea persistente, que sea redundante, que sea oculta y que permita la negación plausible, es decir, quien encuentre un *malware* que se haya colado en la BIOS debe ser incapaz de culpar a quien lo haya desarrollado. Cualquier persona con tiempo puede ser capaz de abrir una puerta trasera y hay gente con el tiempo y la paciencia necesaria para dominar el *firmware* de nuestros sistemas. Actualmente la comunidad científica está realizando un esfuerzo enorme por garantizar que nadie pueda actualizar alegremente el *firmware* de cualquier dispositivo. Existen trabajos recientes que presentan como solución el uso de *blockchain* para permitir la actualización del *firmware* de nodos de sensores a través de la red.

Las arquitecturas y sistemas sobre los que trabajamos y depositamos nuestra confianza, a pesar de que se protegen con *software* avanzado y criptografía, demuestran que sus sistemas de entrada-salida (es decir, lo que los conecta con otros dispositivos) sigue lastrando defectos del pasado. Romper con estos defectos para generar plataformas más seguras supondría romper con la compatibilidad hacia atrás. Antes de usar cualquier dispositivo es recomendable actualizar el *firmware* que usan mediante un *firmware opensource* que pueda ser analizado, estudiado, revisado y comprobado en periodos de tiempo determinados.

Haciendo un ejercicio de imaginación, si el *hardware* lo realiza China, ¿qué le impide a este país introducir *firmware* contaminado? Y si estamos utilizando drones, tarjetas o dispositivos de China, ¿qué impide que este país nos adelante en el desarrollo de tecnología? Y si los ordenadores de los sistemas financieros español o estadounidense utilizan esa tecnología, ¿qué impide que China pueda actuar sobre ellos?

Y a modo de reflexión final, sabemos que *blockchain* es la base sobre la que se sustentan los nodos Bitcoin. Preguntémonos cuántos nodos tiene China, porque a partir del 51% de los nodos se domina una red que puede ser una parte importante del pilar financiero de muchos países. Por lo tanto, vayámonos preparando porque todavía no se ha puesto nombre a lo que nos enfrentamos.

Realidad aumentada. La simulación aplicada a la defensa

Emilio Varela Sieira

Director General de Tecnobit y Director Corporativo de Estrategia y Desarrollo de Negocio del Grupo Oesía

Las Fuerzas Armadas y la universidad son dos elementos esenciales para Tecnobit, toda vez que existimos gracias a que somos capaces de conectar el conocimiento que se desarrolla en la universidad con las utilizaciones y usos que las Fuerzas Armadas requieren.

Tecnobit es una compañía en la que trabajamos unos tres mil doscientos profesionales que anualmente invierte un 7% de la facturación en investigación y desarrollo tecnológico, lo que supone una inversión anual que va entre los dieciocho y los veintiún millones de euros en este capítulo. Somos una empresa 100% española y 100% privada: la compañía pertenece a sus directivos y no está en la bolsa, por lo que somos dueños de nuestro futuro y preferimos utilizar nuestros recursos en hacer avanzar nuestra organización en vez de en distribuir dividendos.

Hace más o menos tres años le dimos un giro estratégico relevante a la compañía, al centrarla en aquellos nichos tecnológicos en los cuales pensábamos que podíamos considerarnos importantes en un futuro a nivel internacional. A través de ejemplos concretos intentaré explicar la manera en que interrelacionamos las necesidades de nuestros clientes con el conocimiento que se genera en la universidad y cómo esto nos está llevando a tocar tecnologías punteras y proyectos punteros a nivel global. Por ello puedo decir que lo nuestro más que un trabajo es una pasión. Las personas que trabajamos en el Grupo Oesía nos divertimos con lo que hacemos porque cada día estamos tocando el desarrollo tecnológico.

En la línea de tratamiento inteligente de la imagen construimos una cadena que va desde el sensor (el ojo, que en este caso es un sensor óptico y electrónico que denominamos optoelectró-

nica) a un dispositivo que es capaz de presentar la imagen o los datos a un ser humano (HMI)[1]. Hemos desarrollado algoritmos de inteligencia artificial que son capaces de procesar la imagen para darle una utilidad a nuestros clientes, en este caso las Fuerzas Armadas. Estamos equipando a los Eurofighters a nivel global con sistemas que son capaces de identificar los objetivos a través de un sensor óptico, esto es, capaces de decir qué tipo de objetivo es y si es amigo o enemigo, capaces de seguirlo y capaces de ordenarlo en función de la amenaza que representa. Y todo eso hecho en un tiempo que resulte operativo para un piloto de caza de combate. Ahora mismo estamos equipando y haciendo *displays* aeronáuticos para el F-18 y vamos a empezar a hacerlos para el nuevo sistema de combate europeo (el FCAS[2]), pues somos una de las cuatro empresas españolas de primer nivel que han sido nominadas. La utilización del grafeno en los sistemas de HMI va a ser muy importante, sobre todo en términos de reducción de peso, lo que es esencial. Ambos son ejemplos de cómo el conocimiento teórico se aplica a realidades concretas de nuestros clientes. Esta capacidad de inteligencia artificial también se está aplicando en el ámbito naval: fragatas como la F-110 llevarán el mismo tipo de algoritmos que ya se están empezando a aplicar en el ámbito terrestre, para que puedan identificar cualquier tipo de amenaza con sensores pasivos.

Otra aplicación que estamos comenzando a desarrollar se corresponde con sistemas activos de protección de vehículos blindados para que sean capaces de identificar una amenaza en tiempo real de tal manera que puedan lanzar una contramedida. Pero los niveles de inversión para desarrollar este tipo de conocimiento son tan elevados que no podemos acometerlo en solitario. Para poder seguir teniendo tecnología española haciendo este tipo de desarrollo nos hemos valido de programas europeos. Hace más de un año montamos una oficina en Bruselas orientada a conseguir fondos y fruto de ello estamos participando en la actualidad en tres importantes programas en colaboración con socios europeos, cosa que podemos hacer porque nos metimos en nichos muy concretos donde somos especialmente competitivos.

1. Interacción persona-ordenador (*Human Machine Interface*).
2. Futuro Sistema Aéreo de Combate *(Future Combat Air System).*

Otro ejemplo lo tenemos en el ámbito de la electrónica embarcada. Estamos desarrollando la primera red de mini-satélites que se va a lanzar en el mundo, formada por mil trescientos equipos. No hablamos de trabajos experimentales o proyectos de I+D sino de proyectos muy concretos de aplicación comercial que van a servir para transmitir la señal de internet. Esta red es una tecnología española desarrollada por nosotros gracias a colaboraciones previas con la universidad.

En el ámbito de las comunicaciones tácticas hemos desarrollado un *software* de radio con una enorme capacidad de ancho de banda que permite aplicar mecanismos de inteligencia artificial en situaciones de combate (transmite muchísima información de manera instantánea, lo que facilita la toma de decisiones en tiempo real) y también hemos desarrollado sistemas de cifrado seguro de comunicaciones, tanto en voz como en datos. Así es como aplicamos el conocimiento a situaciones reales que necesitan nuestros clientes. En estos momentos estamos desarrollando todo el sistema de cifrado del PRS, que es el sistema de geolocalización que utiliza Galileo, con el objeto de que no pueda ser ni escuchado ni manipulado por terceros malintencionados.

De cara al futuro, tenemos que empezar a correlacionar estas aplicaciones con las utilizaciones que se van a producir dentro de treinta años, y eso es nuestra función. Lamentablemente, en ocasiones el sistema de innovación español carece de mecanismos como el que tienen otros países, por lo que las empresas y la universidad debemos ocupar ese espacio.

En el ámbito de la simulación nuestras principales soluciones tienen que ver con la simulación en vivo, es decir, tienen que ver con los elementos que hay que añadir a los medios operativos para poder sustituir el enfrentamiento con fuego real por enfrentamiento con fuego simulado, lo cual facilita el desarrollo de toda una serie de ejercicios y operaciones que permiten entrenar y formar a un coste muy inferior. En cuanto a simuladores virtuales, campo en el que tenemos una cierta competencia tecnológica a nivel global, disponemos del SIMACA[3], cuya existencia se debe al Ejército de Tierra toda vez que nos ha explicado, detallado y guiado en las funcionalidades precisas para que esta solución

3. Simulador de Artillería de Campaña.

esté en el estado del arte en el que se encuentra. Básicamente esta solución simula de manera virtual el funcionamiento de toda una batería de artillería de campaña, lo que permite instruir a sus operadores de manera constante. Este esfuerzo conjunto nos ha permitido colocar esta solución en Brasil (donde tenemos uno de los centros de simulación más importantes que existen en América Latina) y en el Golfo. La exportación se consigue gracias a que tenemos un usuario inicial que nos permite desarrollar nuestros productos hasta llevarlos al estado del arte. Sin esa ayuda, en este caso del Ejército de Tierra, resultaría absolutamente imposible disponer de un producto vendible a nivel global.

El futuro que le vemos a la simulación tiene que ver con la realidad virtual, la realidad aumentada y la realidad mixta. Los tres tipos son aplicados en el adiestramiento, en la identificación, en la visualización de mapas y guiado de rutas y en la ayuda a la toma de decisiones. Los tres últimos casos se aplican a operaciones reales utilizando principalmente realidad mezclada.

PANEL V

LAS NUEVAS INICIATIVAS EN EL ÁMBITO DE LA INVESTIGACIÓN Y DESARROLLO. POSIBILIDADES DE FINANCIACIÓN

Iniciativas I+D+i en el ámbito del Ministerio de Defensa. Posibilidades de financiación por la Dirección General de Armamento y Material

Óscar Jiménez Mateo

Jefe de la Unidad de Planificación y Seguimiento de I+D de la Dirección General de Armamento y Material del Ministerio de Defensa

El Real Decreto 1399/2018, de 23 de noviembre[1], que desarrolla la estructura orgánica básica del Ministerio de Defensa, establece que corresponde a la DGAM planificar y programar las políticas tanto de armamento y material como de I+D así como dirigir su ejecución. Además, la Orden DEF/685/2012 de 28 de marzo establece que la DGAM regula y coordina como interlocutor único las actividades de I+D de sistemas de armas y equipos de interés para la defensa nacional en el ámbito del Ministerio de Defensa. Aparte de los órganos gestores y directivos también se debe de tener en cuenta a los usuarios finales de la tecnología que se desarrolla a través de los proyectos y programas de I+D (entre los que se encuentran todos los ejércitos) y al organismo ejecutor de las actividades de I+D, que es el Instituto Nacional de Tecnología Aeroespacial (INTA).

La I+D de defensa debe ser finalista, es decir, debe contribuir a satisfacer las necesidades de las Fuerzas Armadas apoyando la evolución y obtención en su caso de las nuevas capacidades militares y además debe contribuir a conformar una base tecnológica e industrial potente de la defensa. Esto se consigue básicamente a través de dos instrumentos: el desarrollo de tecnología aplicada a demostradores (lo que conocemos como Investigación Tecnológica) y el desarrollo de unos prototipos que apliquen la tecnología desarrollada previamente.

Las principales directrices para aplicar en el desarrollo de la política de I+D pasan en primer lugar por priorizar las inver-

1. Sustituido posteriormente por el R.D. 372/2020 de 18 de febrero de 2020.

siones internas. Esto ha resultado de extrema importancia en los años que ha durado la crisis de la que estamos comenzando a salir, puesto que se ha tenido que priorizar muy bien a que se dedicaban los escasos recursos que quedaban para atender a las actividades de I+D del Departamento. En segundo lugar, se deben aprovechar las capacidades y los instrumentos externos de financiación que se nos ofrecen tanto a nivel nacional (a través del Centro para el Desarrollo Tecnológico Industrial - CDTI, de la Agencia Estatal de Investigación - AEI y de otros actores) como a nivel internacional y por supuesto europeo, donde ahora se abre un nuevo escenario en el que tenemos que ser capaces de aprovechar los instrumentos de financiación que se nos van a ofrecer. Y una tercera directriz para un buen desarrollo de la política de I+D es que se debe mejorar la explotación de los datos y de todos los resultados de los proyectos tecnológicos que se van consiguiendo. También tenemos que ser capaces de transmitir a la sociedad las ventajas que puede tener en un futuro la aplicación de determinadas tecnologías en nuestras Fuerzas Armadas.

La política de I+D del Departamento está desarrollada en la Estrategia de Tecnología e Innovación del Ministerio de Defensa (ETID). Esta estrategia pretende proporcionar orientación tecnológica y promover la coordinación entre todos los actores de I+D a nivel nacional e internacional que están relacionados con el sector de defensa de forma que seamos capaces de conseguir en un futuro sistemas de armas lo suficientemente potentes que incorporen las tecnologías más novedosas para nuestras Fuerzas Armadas. Esta Estrategia recoge la política de I+D del Departamento, los instrumentos con los que podemos desarrollar esa política y todo el conjunto de actores del panorama nacional relacionados con la I+D de defensa. La última Estrategia, publicada en 2015, incorpora todo el nuevo escenario de cooperación europea y de nuevos instrumentos que se han puesto a disposición del Ministerio para desarrollar su política de I+D (actualmente se encuentra en revisión y se prevé que la actualización se publique a lo largo del año 2020).

La actual estrategia tiene seis pilares o áreas de actuación funcional fundamentales relacionadas con áreas tecnológicas: armas y municiones, sensores y guerra electrónica, plataformas (con toda la subdivisión de tecnologías comunes y plataformas terrestres, navales y aeroespaciales), NBQR, C4I y combatiente. Contempla un

total de setenta y nueve metas u objetivos tecnológicos a los que el Ministerio de Defensa debe destinar financiación para conseguir futuros sistemas de armas que incorporen la última tecnología.

Esta estrategia no está aislada, ya que está integrada en el Plan Estatal de Investigación que forma parte de la Estrategia Española de Ciencia y Tecnología y de Innovación (2013-2020). Y de hecho, en el Plan Estatal de Investigación Científica, Técnica y de Innovación (2017-2020) está contemplada como un documento estratégico del Ministerio de Defensa en el que se mencionan algunos de los instrumentos que ya estaban disponibles a nivel europeo cuando se publicó el Plan, como la Acción Preparatoria para la Investigación en Defensa (PADR)[2]. Estamos, por tanto, inmersos, conectados y coordinados con los diferentes actores del sistema de I+D+i nacional.

Para implementar la política de I+D contamos con tres tipos de instrumentos. El principal son los instrumentos vinculados al desarrollo de nuevas soluciones tecnológicas, que son los programas y proyectos de I+D del Ministerio de Defensa tanto a nivel nacional como a nivel internacional (desde hace varios años se participa en proyectos colaborativos de la Agencia Europea de Defensa). Otros instrumentos son los vinculados a la coordinación y cooperación en I+D. A este respecto estamos en coordinación con diferentes actores nacionales (como pueden ser el CDTI y la AEI) y con agencias regionales (como puede ser la Agencia IDEA[3]). Además estamos participando en los paneles tecnológicos STO de la OTAN. También participamos con representantes en los grupos tecnológicos CapTech de la Agencia Europea de Defensa, cuya misión es promover el desarrollo de proyectos en cooperación que aporten soluciones a las áreas de interés de cada nación. El tercer tipo de instrumentos son los vinculados al conocimiento tecnológico mediante los cuales se difunden los distintos resultados que se van obteniendo. Esto se hace a través del Sistema de Observación y Prospectiva Tecnológica de la DGAM, que periódicamente publica tanto monografías como boletines trimestrales y se encarga de organizar el Congreso Nacional de I+D en Defensa y Seguridad. También se mantiene un portal de

2. *Preparatory Action on Defence Research.*
3. Innovación y Desarrollo de Andalucía.

tecnología e innovación para difundir los resultados que se van obteniendo y poner en conjunto a todos los actores nacionales relacionados con la I+D+i.

Las necesidades de I+D que se identifican por los diferentes actores implicados en la I+D de Defensa, incluidos los ejércitos y usuarios finales de la tecnología, tienen que ser integradas en el planteamiento del Ministerio de Defensa. Tal y como establecen las instrucciones, se debe generar en origen un documento de necesidad operativa en caso de que esa necesidad esté asociada a una capacidad militar o una necesidad de las Fuerzas Armadas, o un documento de necesidad funcional en el caso de que la necesidad se identifique desde otro tipo de objetivo más a medio o largo plazo, que se identifiquen algunas tecnologías que hay que potenciar para obtener futuros sistemas de armas competentes o que surjan posibilidades de cooperación a nivel internacional. Las necesidades se integran en el Sistema de Planeamiento y Programación y de esta forma se van convirtiendo en un proyecto concreto de I+D. El sistema debe ser suficientemente flexible, toda vez que pueden aparecer necesidades que no estaban contempladas en programación y que deben ser atendidas, tales como oportunidades de colaboración. A partir de 2018 nuestras actuaciones están incluidas en el Programa de Actuación Anual que edita el Ministerio de Ciencia e Innovación en el marco del Plan Estatal de Investigación Científica y Técnica y de Innovación 2017-2020.

Los instrumentos que tenemos para materializar esos programas y proyectos de I+D en la inversión pública son dos programas de gasto asociados a la I+D de Defensa: el programa de gasto 464A de Investigación y estudios de las Fuerzas Armadas y el Programa 464B de Apoyo a la innovación tecnológica en el sector de la defensa. La diferencia entre ambos estriba en que el primero se gestiona directamente desde el Ministerio de Defensa y el segundo, que está pensado para conceder préstamos prefinanciación de grandes desarrollos tecnológicos de las Fuerzas Armadas, lo gestiona el Ministerio de Industria. En general, el programa de gasto que gestiona Industria está orientado a grandes industrias del sector, a grandes proyectos de desarrollo y a niveles de madurez tecnológica más altos. El programa que gestiona el Ministerio de Defensa normalmente se materializa a través de contratos, la mayor parte de ellos plurianuales (por la propia característica de

la I+D), y están orientados a satisfacer necesidades de las fases y fomentar la base tecnológica. En general, está dedicado a niveles de madurez más bajo. Conforme a los últimos Presupuestos Generales del Estado (PGE) publicados en 2018, el programa 464A tuvo una dimensión económica de unos dos cientos once millones de euros, de los cuales unos ochenta y cinco corresponden a inversiones reales, y la dimensión económica del programa de gasto 464B rondó los cuatrocientos sesenta y ocho millones de euros.

En 2019, la Dirección General de Armamento y Material ha tenido activos alrededor de treinta y cinco programas relacionados con plataformas terrestres, armamento y munición, NBQ, sensores y guerra electrónica, programas europeos, plataformas aéreas, plataformas navales (programas tecnológicos de la fragata F-110 que no se atienden desde nuestro presupuesto pero acaban repercutiendo en el programa de gasto del Ministerio de Defensa), comunicaciones, ciberseguridad, etc. Por destacar alguno, el programa Galileo PRS por el que la Dirección General apostó muy fuerte para apoyar a la industria del sector y al que se está apoyando desde hace dos o tres años mediante campañas que permitan validar el receptor nacional que ha desarrollado la industria nacional. En cuanto a nuestra participación en programas europeos a través de la Agencia de Defensa Europea, participamos en los Programas de inversión conjunta (JIP)[4], en los que a través de convocatorias competitivas hemos podido colocar a la industria del sector y hemos obtenido muy buenos resultados. En todos los programas de este tipo (relacionados principalmente con protección de la fuerza, conceptos innovadores de tecnología y NBQ) se ha tenido un retorno por encima del 100%. De hecho, en el último (el JIP-CBRN) se ha obtenido un retorno del 170% de la inversión que puso el Ministerio de Defensa. Ha sido una forma de empezar a poner esas pequeñas semillas para que nuestra industria sea competitiva en el marco europeo.

Cabe destacar el Programa COINCIDENTE, mediante el cual se pretende aplicar tecnologías que han sido desarrolladas en el ámbito civil a demostradores o prototipos que pueden ser de utilidad para el Ministerio de Defensa. Nació en 1986 y desde 2010 sus convocatorias están reguladas por el BOE. En las últimas con-

4. *Joint Investment Program.*

vocatorias se ha delimitado a temáticas concretas el alcance de las propuestas a presentar. El esfuerzo económico que el Ministerio ha dedicado a este programa desde su origen ha sido de cuarenta y ocho millones de euros hasta 2017. Teniendo en cuenta las dos últimas convocatorias (2018 y 2019), dicha cifra se eleva a los sesenta millones de euros que se han dedicado a alrededor de doscientos treinta proyectos de I+D. Cabe decir que Andalucía es una de las comunidades más activas, tanto presentando propuestas como en proyectos concedidos. La temática de las últimas dos convocatorias son amplias y diversas. En la convocatoria de 2018, que ya está resuelta y se encuentra actualmente en fase de contratación, se han seleccionado veintidós proyectos de temáticas tales como armas de energía dirigida láser, guiado de municiones, robótica, detección y neutralización de IED, protección pasiva del combatiente y de plataformas, protección NRBQ, sistemas inteligentes de análisis y explotación informática y ciberdefensa. En la convocatoria de 2019, que está en proceso de evaluación, destacan proyectos en el campo del empleo innovador de RPAS, de la simulación aplicada a problemas militares y de la información y comunicaciones submarinas aplicadas a misiones militares.

En cuanto al futuro de la I+D, resulta obvio decir que pasa por el nuevo EDF en sus dos dimensiones: la ventana de investigación y la ventana de capacidades.

Iniciativas en el ámbito de la investigación y desarrollo en proyectos de defensa. Nuevas iniciativas europeas de financiación

Alfonso Azores García

Coronel Responsable del Área de Cooperación Multilateral de la Dirección de Armamento y Material del Ministerio de Defensa

Cuando hace año y medio me incorporé a la DGAM, solíamos decir que algo se estaba moviendo en Europa. La bella durmiente, que es como se identificó en Lisboa hace diez años a la política de seguridad y defensa europea, estaba empezando a desperezarse. Hoy en día puedo afirmar, sin miedo a equivocarme, que algo ya está en marcha, que el tren ha salido de la estación, y que cuanto antes seamos capaces de entender cómo funciona, qué supone, de adaptar nuestras estructuras y de adaptar también nuestra forma de trabajar, tanto a nivel del Ministerio de Defensa como de la industria, mejor estaremos posicionados para el futuro.

Un informe reciente de la Comisión Europea concluía que a pesar de que la Unión en su conjunto se situaba como el segundo contribuyente en gasto de defensa a nivel mundial (tras los Estados Unidos), el gasto que realiza es ineficiente, debido a la fragmentación en distintos sistemas de armas que conduce a duplicidades en el gasto y a dificultades de interoperabilidad de los materiales. El informe establecía que el 80% de la inversión en defensa se realizaba dentro de las propias fronteras de cada uno de los países de la Unión, lo cual se traducía en un gasto ineficiente del orden de veinticinco mil a cincuenta mil millones de euros anuales.

En los últimos dos o tres años la percepción que los europeos tienen de la necesidad de invertir en defensa ha cambiado. Rusia ha vuelto otra vez al escenario, nos enfrentamos a los problemas de las migraciones a Europa, al terrorismo internacional y al auge de los nacionalismos euroescépticos que han ido surgiendo en los países de la Unión y que cuestionan sus propios cimientos. Estos y otros problemas han hecho que sobre la seguridad y defensa

se haya construido una oportunidad de cimentar el concepto de Europa.

El que fuera presidente de la Comisión Europea, Jean-Claude Juncker, decía que había llegado el momento de que Europa asumiera sus propias responsabilidades en materia de defensa. Y eso, bajo el paraguas de una nueva estrategia de la Unión en los últimos dos años, se ha plasmado básicamente en dos iniciativas. Una iniciativa es la PESCO, que podemos identificar como el motor político de esta nueva Europa, y cuya finalidad fundamental no es otra que favorecer el que los países miembros lleguemos a acuerdos en cuanto al desarrollo de capacidades militares. Y otra iniciativa muy potente, a la que podemos denominar como motor económico, es el Plan de Acción Europeo de la Defensa (EDAP)[1]. Ambas iniciativas son incentivos para la cooperación, que no buscan otra cosa que forzar que los estados miembros y las industrias de defensa de Europa se pongan de acuerdo para definir requisitos y para adquirir capacidades.

Centrándonos en el EDAP, si bien es cierto que la política de I+D de nuestro Ministerio de Defensa es finalista, la DGAM ha introducido una excepción en el tratamiento del EDF con una triple finalidad: contribuir al desarrollo de una base industrial y tecnológica sólida y competitiva que permita que nuestra industria de defensa esté situada en las mejores condiciones en los próximos veinte o treinta años, satisfacer la necesidad de capacidades militares nacionales integrándolas con las del resto de los países miembros y colaborar en la mejora de la autonomía estratégica de la Unión en su conjunto.

Desde la DGAM hemos entendido que algo ha cambiado y ello exige un cambio de mentalidad. Para poder ser capaces de tener unas capacidades comunes, primero tenemos que ser capaces de tener una industria que ha entendido el nuevo proceso y que tiene la capacidad tecnológica y organizativa de integrarse en estructuras europeas de consorcios de programas futuros. Si no conseguimos que nuestra industria vaya por delante en este proceso, nunca alcanzaremos la finalidad última, que es adquirir esas capacidades militares.

El EDAP se articula a través de tres pilares fundamentales: el EDF, que representa la financiación pura del presupuesto de

1. *European Defence Action Plan.*

la Unión a proyectos de I+D de Defensa; el refuerzo de un mercado único de defensa en Europa; y el fomento de la cadena de suministro, un aspecto fundamental para España. España es un país en el que el tejido industrial está fundamentalmente basado en pymes. Por lo tanto, el hecho de que Europa apueste por el desarrollo y el apoyo a estas empresas es una oportunidad que nuestra industria debe saber aprovechar.

Respecto al EDF podemos decir que por primera vez la Unión Europea pone financiación para el desarrollo de proyectos de I+D en el ámbito de la defensa. Estamos hablando de la PADR, que aporta 90 millones de euros para proyectos de desarrollo desde 2017 a 2019, y del Programa Europeo de Desarrollo Industrial en materia de Defensa (EDIDP)[2], de dos años de duración (2019-2020), que aporta quinientos millones de euros. Ambas iniciativas suponen una fase de prueba: la Unión Europea está aprendiendo, y pone en marcha unas cantidades limitadas de financiación para que tanto los países miembros de la Unión, como la propia Comisión y la industria europea empiecen a practicar y a entender las bases de este nuevo sistema.

A partir de 2021 la Comisión Europea tiene previsto poner en juego trece mil millones de euros en el periodo temporal del 2021-2027. De esos trece mil millones de euros España ya ha pagado un porcentaje importante a través de las aportaciones hechas al presupuesto de la Unión para el desarrollo de políticas de seguridad común, políticas migratorias, empleo, sostenibilidad, etc. Un porcentaje que, cuando se materialice el Brexit, se estima que estará en torno al 9%, por lo que estamos hablando de cerca de ciento noventa millones de euros anuales que deberíamos ser capaces de recuperar, porque de hecho ya los hemos pagado, o de lo contrario significaría que algo no estaríamos haciendo bien.

Es importante señalar que la Comisión establece unas condiciones de elegibilidad que son de aplicación a las entidades que optan a esta financiación (empresas públicas o privadas, universidades y centros de investigación radicados en territorios de la Unión), siendo una de ellas la obligatoriedad de establecer consorcios: para que un proyecto reciba la correspondiente subvención tiene que ir de la mano de al menos otras dos entidades

2. *European Defence Industrial Development Program.*

ubicadas en dos países distintos de la Unión y debe tener el apoyo de al menos dos o tres ministerios de defensa. Y también establece un sistema de bonificaciones que va desde actividades de diseño (que pueden alcanzar el 100% de bonificación) hasta actividades de prototipo (que alcanzan un 20%) o de certificación de prototipos (que pueden oscilar entre el 65 y 70%).

Por lo tanto, con el EDF se nos presenta un desafío y una oportunidad. Representa una oportunidad para que el Ministerio de Defensa obtenga una financiación que no recibe vía presupuestos. Cabe recordar que nuestro presupuesto de defensa para I+D ronda los veinte millones de euros, siendo uno de los más bajos de la Unión. Si hacemos bien las cosas, podremos recibir una financiación externa para desarrollar nuestros propios proyectos de I+D (recordemos los ciento noventa millones de euros anuales como objetivo de retorno).

Pero también es un desafío, porque con este sistema de bonificaciones la Comisión no cubre el 100% del coste de los proyectos. Se estima que como media puede cubrir entre un 40-45% de su coste real, por lo que el resto tiene que venir de la industria o de los países miembros. Quiere decir que, para recuperar ciento noventa millones del EDF se debe movilizar en torno a un 50% adicional, que son prácticamente otros ciento noventa millones de euros cada año procedentes del presupuesto o de la industria. Ese es el gran desafío al que nos enfrentamos actualmente.

En este sentido, en el Ministerio de Defensa se han adoptado medidas en dos áreas: una interna, dirigida a preparar y a adaptar a este nuevo desafío tanto a la administración civil y militar como a la industria, y una externa, dirigida a posicionarnos como nación y a posicionar a nuestra industria de defensa en el núcleo del nuevo escenario europeo.

Como medida de carácter interno cabe señalar el cambio de mentalidad que se ha fraguado gracias a la tremenda labor divulgativa que se ha hecho para que los actores que están implicados en este proceso entiendan realmente lo que nos jugamos. Estamos en un punto de inflexión y en una encrucijada que va a marcar los futuros veinte años de la industria de defensa en Europa. Si no jugamos bien las cartas nos quedaremos fuera de una oportunidad que España ni debe ni puede dejar pasar. A este respecto ya hemos establecido unos niveles de coordinación que han sido muy beneficiosos. Entre otros, se ha creado un grupo de trabajo

interministerial con representantes de Industria, de Exteriores, de Defensa, de Economía y de Hacienda que se reúne periódicamente con las asociaciones industriales de defensa para analizar y evaluar esas iniciativas y ver cómo podemos responder de la mejor manera posible.

En cuanto a medidas de carácter externo, hemos posicionado personal español en la dirección general correspondiente de la Comisión Europea que gestiona estas nuevas iniciativas (DG GROW)[3], lo que nos permite conocer de primera mano la visión de la propia Comisión para poder adaptarnos y buscar soluciones alineadas con la idea de financiación. Junto con Francia, Italia y Alemania hemos creado, a iniciativa española, un grupo de influencia (Grupo E4) en el ámbito de la Comisión, que se reúne con cierta periodicidad para buscar posiciones de fuerza, toda vez que somos los cuatro principales contribuyentes al presupuesto del EDF. Y por último, hemos intentado presentar nuestra industria poniendo en valor sus capacidades y la fiabilidad de su tecnología. En mayo de 2018 se organizó por primera vez una feria industrial de defensa en IFEMA, con vocación de continuar en el futuro, a la que se invitó a la industria y los ministerios de defensa de varios países, para que pudieran coordinarse y llegar a esos necesarios acuerdos, que abrirán las puertas a la financiación europea.

En el período de prueba del EDIDP, España ha conseguido presentar diecisiete proyectos, de los cuales cinco están bajo liderazgo español, todos ellos apoyados y financiados parcialmente por el Ministerio de Defensa. Lo realmente importante de esto es que en diecisiete consorcios industriales hay representación de la industria nacional (en la llamada de ofertas que cerró la Comisión el 30 de septiembre de 2019 se presentaron cuarenta proyectos procedentes de los veintisiete países de la Unión). Independientemente del resultado de la evaluación de los proyectos (que no se sabrá hasta después de enero de 2020) considero que ya hemos ganado, porque nuestra industria está ahí, lo que quiere decir que ha aprendido y entendido la necesidad de buscar consorcios y de

3. *Directorate-General for Internal Market, Industry, Entrepreneurship and Small and Medium-Sized Enterprises*. Dirección General para el mercado interno, industria, emprendedores y pequeñas y medianas empresas.

posicionarse para buscar su sitio en el ámbito industrial internacional. De hecho, ya hay industrias que no se plantean acceder a ningún tipo de desarrollo sino van de la mano de su homóloga italiana, alemana o checa, lo que es un gran paso adelante. Si conseguimos que se adjudiquen los proyectos presentados en EDIDP 2019 en los que esté inmersa la industria española, el retorno esperado a la industria nacional es de unos noventa millones de euros. Estamos hablando de multiplicar prácticamente por cuatro el 9% que nos marcamos como objetivo de retorno del Fondo, lo que supone cerca de un 35% de retorno efectivo. El desafío al que nos enfrentaremos cuando hablemos de mil setecientos millones anuales es poder presentar proyectos que estén a la altura para mantener ese retorno del 9%, y sinceramente creo que tenemos la capacidad para ello.

En cuestión de defensa, la Unión Europea ha venido para quedarse y para transformar nuestra industria, y cuanto antes lo asumamos, mejor será para todos. En septiembre se anunció la creación de una nueva Dirección General de Defensa y Espacio, lo que significa que los países miembros hemos cedido de nuevo soberanía y responsabilidades en beneficio de la Comisión Europea, al igual que ya hicimos en otros ámbitos de la Unión. En el Ministerio de Defensa seguimos esa misma línea. Aunque nuestro presupuesto de defensa sea muy limitado, España no puede renunciar a ser un actor clave, toda vez que será la cuarta economía de la Unión después de que se materialice el Brexit. Esto va a exigir, como ya he señalado, una adaptación de la administración civil, militar y de la industria, y estamos en ello. La industria ha reaccionado muy bien; quizás sea más complicada la adaptación de la administración militar. Hay que revisar el proceso de planeamiento de capacidades porque hay unos nuevos *input* que habrá que tener en cuenta. Tenemos que ser conscientes de que los fondos están ahí. Los españoles ya hemos pagado el 9% de los trece mil millones, y si no los recupera nuestra industria, los recuperará la industria de otro país. Ese es el reto al que nos enfrentamos.

Iniciativas en el ámbito de investigación empresarial. Posibilidades de financiación

Daniel Mosquera Benítez
Jefe del Área de I+D+i de la Dirección de Desarrollo de Negocio de la Ingeniería de Sistemas para la Defensa de España

Hemos visto que existe un contexto de financiación europea que nos está moviendo y que va a lograr que de alguna manera centralicemos capacidades para vincularlas con la Fuerza 35 de cara a conseguir la fuerza de ventaja, que es el objetivo último. Tenemos escenarios globales y nuevas amenazas, lo cual supone la evolución de los ejércitos e implica una necesidad tecnológica que pasa por una potenciación del I+D+i que necesita financiación.

En ISDEFE hemos entendido que tenemos que jugar en Europa en lo que personalmente defino como las «pandillas del I+D+i», porque hemos pasado de una situación en la que creíamos que podríamos obtener objetivos yendo por nuestra cuenta a otra en la que tenemos que buscar a «dos colegas» de dos Estados Miembros diferentes para poder acceder a los fondos. El abanico que tenemos de todo el EDF es muy amplio: tenemos una ventana de investigación con programas como la PADR y tenemos la ventana de desarrollo de capacidades con la política de desarrollo industrial. Esto nos tiene que llevar a la adquisición de capacidades. También tenemos unas prioridades de desarrollo de capacidades que han sido recientemente definidas por la EDAP, que nos van dando pistas de por donde tenemos que ir.

El EDF fue creado para promover la cooperación tecnológica entre estados miembros, siendo esta una de sus funciones. Es cierto que la PADR es un primer paso para demostrar el valor añadido que tiene el programa de la investigación, pero pretende profundizar e incrementar la colaboración entre los distintos Estados Miembros. El programa de desarrollo industrial no es la excepción, se trata de cooperar y desarrollar entre todos. Pero el sistema de acceso a los fondos no deja de ser competitivo, lo

que significa que aunque nos aliemos en consorcios tenemos que luchar entre nosotros, porque al final solamente una propuesta puede tener éxito. ¿Y qué pasa cuando hay dos propuestas que por sí no son lo suficientemente buenas pero la unión de ambas sí lo es? ¿Qué pasa cuando tenemos una propuesta que tecnológicamente es disruptiva pero le falta el área de conocimiento que tiene la otra? ¿Acaso tenemos mecanismos para reconocer lo bueno de las dos y tener una buena iniciativa o una iniciativa potente de I+D+i?

En la actualidad se está trabajando en las funciones de combate de la Brigada 2035. En cuanto a inteligencia artificial, el EDAP está invirtiendo en hacer prospectiva tecnológica y en ver a dónde nos va a llevar su aplicación o qué capacidades va a permitir incrementar. Recientemente se han celebrado unos *workshops* en los que ha participado gran parte de Europa y en los que entre otras cosas se ha definido una hoja de ruta. En paralelo se publicó y se cerró el premio a la innovación, que tiene una componente de aplicación de la inteligencia artificial en defensa. Si pensamos en la PADR, recientemente se ha cerrado la tercera convocatoria. La primera se enfocaba, entre otras cosas, en la prospectiva tecnológica. La segunda trataba sobre tecnologías que son críticas y no están en nuestras manos (la Comisión Europea ha querido identificarlas y proponer hojas de ruta para desarrollarlas en Europa). En la tercera convocatoria ahonda ya en los temas de tecnologías disruptivas, y entre ellas la inteligencia artificial aplicada al mando y control, por ejemplo, que es una de las capacidades que va a requerir la Brigada 2035. Esto significa que ya están en marcha unas cuantas actividades de las cuales podemos aprovecharnos. Es verdad que tenemos que retornar el dinero que España ya está poniendo, pero creemos que antes debemos asegurarnos de que en esos programas estén las necesidades de la brigada de nuestro Ejército, de modo que el retorno sea efectivo tanto desde el punto de vista de la inversión como desde el punto de vista de las capacidades que realmente debemos tener.

Las claves están en que la I+D sea finalista. Tenemos que colaborar no solo porque nos lo exijan los fondos europeos sino porque juntos somos más fuertes. Costará romper la inercia pero debemos entender que remando juntos lo conseguiremos. No olvidemos que el 80% de los ciudadanos europeos ya comprende que son necesarias capacidades propias de defensa, por lo tanto ya

se ha dado un gran paso. Aunque reconozcan que no ven claro un ejército europeo, ya reconocen que debemos trabajar juntos para desarrollar esas capacidades. Aprovechemos los fondos disponibles desde dos perspectivas: desde lo que ya se está desarrollando en otros campos (un ejemplo claro de coordinación entre la PADR y los fondos de seguridad del programa Horizonte 2020 es la investigación que se está llevando a cabo en el uso de plataformas autónomas) y desde el punto de vista de los fondos propios de I+D en ISDEFE. Ambos son modestos, pero quizás una suma de fondos modestos pueda llegar a representar algo de envergadura.

Otra cuestión de importancia es entender que es fundamental liderar estos procesos. Si bien es cierto que estar en tantos proyectos de la PADR puede considerarse una misión cumplida, no lo es menos que lo realmente importante es liderarlos. La mejor manera de posicionar nuestros intereses y las necesidades de la Brigada 2035 es liderar proyectos allá donde se juegue cada euro en Europa. Y liderar solo se logra asumiendo el riesgo, la incertidumbre y también el fracaso (en ocasiones, no dar con la solución también es dar con ella, pues sabemos por donde no deben ir los tiros).

Recientemente ISDEFE ha iniciado una colaboración con el MADOC en el ámbito de la investigación. Nos ponemos a su disposición y para ello necesitamos dos cosas: necesidades y financiación. Las necesidades están claras. En cuanto a la financiación, hay dos maneras de conseguirla: buscarla fuera o poner lo que tenemos optimizando cada euro. Desde el punto de vista de la innovación vamos a contribuir al análisis de las tendencias en el empleo de la inteligencia artificial en el ámbito militar y su aplicación al entorno operativo terrestre de la Brigada 2035, para lo que partiremos de lo que están haciendo nuestros aliados. A este respecto, en Francia hablan de la innovación abierta y sin filtros, es decir, sin capar las ideas de la base. Si tenemos ideas dejemos que fluyan; luego será cuestión de dinero el poder ejecutarlas o no. Pero es bastante posible que las grandes ideas, los grandes productos o los grandes posicionamientos hayan empezado de una idea que no ha tenido filtros. En el Reino Unido hablan de no dejar a nadie atrás. La doctrina del uso de la tecnología debe ser algo que esté presente desde el punto de vista conceptual: disponer de un sistema que no sabemos operar puede ser tan bueno o tan malo como no tener ninguno. En los Estados Unidos

resaltan su vocación de involucrar a tanta gente como sea posible en la fase conceptual de todos los ejercicios, lo que es muy importante porque de esa manera se logran, al menos, dos cosas: una, que la tecnología o el concepto de la doctrina que se desarrolle sea entendida y querida por todos; y otra, que los tiempos de respuesta sean mucho menores tras su implantación. En cuanto a la aportación española en este ámbito cabe destacar la importancia de generar confianza en el contorno y en el contexto.

Para cerrar el ciclo, se debe colaborar para definir y potenciar las capacidades que necesitamos. Si la financiación está en Europa tendremos que ser lo suficiente astutos, lo suficientemente rápidos y estar lo suficientemente agrupados para poner las necesidades de nuestra brigada en Europa. Con eso lograremos tres cosas: una, encontrar la financiación que necesitamos; dos, traer el retorno; y tres, ser efectivos. Todo ello para conseguir el objetivo final: la fuerza de ventaja.

Desarrollo industrial

Cecilia Hernández Rodríguez
Departamento de Grandes Instalaciones y Programas Duales del Centro para el Desarrollo Tecnológico Industrial

El CDTI tiene fondos propios que le permiten financiar a empresas, que además se complementan con los PGE y con fondos europeos. Desde 1977, año de su creación, ha movilizado más de veinticinco mil millones de euros y más de trece mil empresas se han beneficiado de las ayudas del Centro. En la actualidad dispone de algo menos de mil millones de euros anuales en financiación directa. Además, el Centro favorece que España retorne fondos de programas en los que participa, como son los Programas Marco de Investigación y Desarrollo Tecnológico e Innovación de la Unión Europea (Horizonte 2020 en su edición actual y Horizonte Europa en el periodo 2021-2027), la Agencia Europea del Espacio, u otros Programas de Espacio y Grandes Instalaciones Científicas Internacionales.

La financiación del CDTI se dirige empresas que realicen I+D+i de cualquier sector, lo que incluye Defensa, si bien hasta ahora no se contemplaba de manera específica. En la última reestructuración del CDTI (noviembre de 2018) se creó la Dirección de Espacio, Grandes Instalaciones y Programas Duales enfocada a potenciar la industria de alta tecnología. Y dentro de ella se estableció el Departamento de Grandes Instalaciones y Programas Duales.

Desde este departamento, el CDTI alinea sus actividades con el sector de la Seguridad y la Defensa, enfocándolas hacia las necesidades reales que se tienen en estos ámbitos a la vez que se garantiza su aplicación dual. En este corto periodo se ha puesto ya en marcha un protocolo de colaboración entre los Ministerios de Ciencia e Innovación y de Defensa. En ese protocolo, CDTI figura como actor fundamental que va a coordinar su financiación nacional con el Ministerio de Defensa y al que además va a

apoyar en programas europeos y grandes programas estratégicos internacionales.

Los beneficiarios de la financiación del CDTI (fundamentalmente empresas, ya sean grandes o pymes) pueden ejecutar sus proyectos de forma individual o en consorcios nacionales e internacionales (de estos últimos, CDTI cubre la parte española). El resto de los actores del ecosistema I+D+i puede participar bajo la figura de subcontratación. La excepción ha sido la convocatoria Cervera de subvención a Centros Tecnológicos que se publicó en 2019.

Por lo que respecta a los diferentes instrumentos, los proyectos más tradicionales y característicos del CDTI son los de I+D en convocatoria abierta. Éstos se evalúan de forma interactiva y se propone para su aprobación al consejo de administración del Centro, que se reúne con periodicidad mensual. Otras tipologías de proyectos, como son los de Innovación y cuyo foco es la adquisición de tecnologías, también responden a convocatoria abierta. Esta ventanilla supone otorgar de forma estable y permanente ayudas con tramo reembolsable y tramo no reembolsable. Además, CDTI también gestiona convocatorias competitivas que se ajustan a la Ley de Subvenciones.

Una de las fortalezas del Centro es que la evaluación, tanto desde el punto de vista técnico como financiero, se hace con personal propio. CDTI además ofrece a la empresa la posibilidad de solicitar de forma gratuita informes motivados que son vinculantes para desgravaciones fiscales por inversión en I+D. Otro tipo de actividad que también cubre el CDTI es el apalancamiento de capital riesgo.

Centrándonos en acciones específicas para el desarrollo de tecnologías duales, se ha adaptado el instrumento de financiación de I+D para que estos proyectos tengan el máximo tramo no reembolsable que concede el Centro (33%). Además, las pymes se beneficiarían de una minoración del 70% de las garantías que pudieran requerirle en función de su situación financiera. Cabe destacar que cuando la empresa opta por esta tipología permite al CDTI consultar al Ministerio de Defensa y/o Interior durante el proceso de evaluación.

Por lo que respecta a las políticas de la Compra Pública Innovadora, que suscitan mucho interés, conviene recordar que el CDTI ha sido partícipe de su puesta en marcha desde sus orígenes, por un lado con el instrumento INNODEMANDA (*fast track* en la evaluación de proyectos de I+D del CDTI ligados a contrata-

ción pública) y por otro facilitando la colaboración a escala europea, pero sin ejecutar la compra. En 2019, como novedad y tras la creación de una Oficina de Compra Pública, se pone en marcha un instrumento de Compra Pública Precomercial (CPP) que permite al CDTI adquirir un prototipo que posteriormente se cede a una administración usuaria. La administración receptora, con la cual se firma un convenio de colaboración, valida y colabora en la gestión del proceso. Se prevé utilizar fondos FEDER, lo que limita las áreas geográficas que se pueden beneficiar. El desarrollo de estos prototipos debe realizarse en un periodo máximo de dos años, en el cual las tecnologías deben alcanzar la validación del prototipo en entorno real. El volumen presupuestario mínimo debe ser de dos millones de euros. El proceso de la CPP se inició habilitando una convocatoria de ideas que cerró el 31 de mayo del 2019 con el objeto de establecer un repositorio. De ellas, se seleccionaron las que se consideraron más viables, previa consulta con las administraciones potencialmente receptoras del prototipo. A continuación se abre una consulta pública al mercado para definir la licitación, y posteriormente avanzar en el proceso de desarrollo hasta ultimar la compra y cesión.

En lo referente al entorno europeo, el CDTI apoya con su experiencia al Ministerio de Defensa en el ámbito de los Programas de Defensa de la Unión Europea (EDF y sus precursores PADR y EDIDP).

Si analizamos la historia de los Programa Marco de la UE, al principio los retornos españoles quedaban por debajo de la contribución española a los presupuestos de la Unión y muy pocos proyectos eran liderados. Por el contrario, actualmente se ha alcanzado una posición de justo retorno y liderazgo, incluso por encima de nuestra aportación en términos porcentuales en algunos programas en los que alcanzamos primeras posiciones. Estamos convencidos de que en el futuro programa de defensa podremos incorporar muchas de las lecciones aprendidas y cosechar buenos resultados, como está ya ocurriendo en la PADR.

Toda la información del CDTI está disponible en página web del Centro https://www.cdti.es, desde donde además se puede realizar la suscripción a listas de distribución específicas para programas y tecnologías duales (https://www.cdti.es/index.asp?MP=8&MS=69&MN=2&r=1188*668). También se puede seguir al CDTI en redes sociales (@CDTIoficial).

Iniciativas de investigación tecnológica industrial en Andalucía

Fabián Varas Sánchez
Director Técnico de Corporación Tecnológica de Andalucía

Corporación Tecnológica de Andalucía (CTA) es un modelo de colaboración público – privado singular que sigue las iniciativas similares a las JTI[1] a nivel europeo. Es una fundación privada que lleva catorce años ayudando a innovar a empresas de diferentes tamaños y sectores, centros de generación de conocimiento, universidades y también a administraciones públicas.

CTA es un *cluster* empresarial conformado a día de hoy por ciento sesenta y cinco empresas que realizan actividades de I+D+i en Andalucía. Tiene capacidad de financiación propia, esto es, financia actividades de I+D+i empresariales con fondos de carácter privado. Presta servicios de apoyo e innovación a aquellas entidades de diferentes tipos que por distintas razones no pueden ser miembros de pleno derecho de la fundación.

Es un modelo muy singular, básicamente centrado en conformar una alianza entre las empresas, las universidades y la Administración (la famosa triple hélice). Se podría decir que somos «la materia que engrasa» los diferentes engranajes de esas tres instituciones para intentar que funcionen lo mejor posible. Nuestro foco está puesto en que los proyectos de I+D+i sean económicamente viables. La I+D+i tiene que notarse en la cuenta de resultados, lo que desde el punto de vista empresarial es fundamental, porque de no ser así una empresa sería incapaz de seguir adelante desarrollando actividades de I+D+i. Como *cluster* empresarial y nexo de unión promovemos muchísimo la colaboración competitiva y las sinergias. Para CTA el tema de innovación abierta ha quedado ya un poco desfasado. Hablamos de la innovación colaborativa,

1. *Joint Technology Initiatives* (Iniciativas tecnológicas conjuntas).

ecosistemas y de otros modelos más avanzados en los cuales se está demostrando que también el Ministerio de Defensa y otras administraciones están apostando como modelos de promoción de la innovación. Trabajamos a la medida de las necesidades de las empresas ofreciendo una serie de servicios. Somos el principal financiador privado de I+D+i de España y uno de los principales a nivel europeo. Sin embargo, como proporcionamos financiación a la I+D+i se nos considera una organización pública en no pocas ocasiones, y es por eso que somos tan singulares.

Nuestro objetivo es muy sencillo: queremos incrementar la competitividad de las empresas. Obviamente, hay muchas formas de conseguirlo. Nosotros creemos que la vía más adecuada en el largo plazo es la diferenciación a través de actividades de I+D+i. Dentro de ese esquema de colaboración de ecosistemas o de innovación abierta somos cada día más conscientes de que no se puede tener todo el conocimiento, como bien sabe el Ministerio de Defensa. Cada vez es más necesario transferirlo desde los centros de generación a las universidades y empresas y también desde las empresas a las universidades.

Somos una entidad multisectorial, pero no tenemos área de defensa y no tenemos programas duales (como sí tiene el CDTI). Pero, ¿qué es un proyecto de I+D+i y qué sector se puede encajar en una determinada temática? A día de hoy consideramos fundamental lo que nosotros llamamos la hibridación de las tecnologías. Es esencial que dentro de un proyecto haya multidisciplinaridad, porque solo de esa forma se pueden llegar a conseguir los objetivos verdaderamente ambiciosos que muchas veces se plasman. Y por lo tanto, lo que nosotros hacemos es poner el conocimiento de diversos sectores alrededor de la empresa para que pueda ir más allá del que tiene de manera natural.

Básicamente CTA lleva a cabo una serie de actividades de promoción, colaboración, relación, difusión y comunicación de resultados. Pero también hace programas de innovación abierta, apoya en la compra pública e innovación (tenemos un convenio con la Guardia Civil en este sentido), desarrolla estrategias de I+D+i, apoya a movilizar y definir proyectos, a generar planes de trabajo, a buscar no solo nuestra financiación sino aquella que sea más adecuada para el proyecto, ya sea de CDTI o de cualquier otro organismo, etc.

Por dimensionar la organización en cifras, CTA se diferencia del CDTI de manera evidente: el CDTI es el hermano mayor en

cuanto a financiación en España y nosotros somos el hermano pequeño de Andalucía. Somos ciento sesenta y cinco empresas. A lo largo de estos catorce años de actividad hemos promovido más de tres mil proyectos, de los cuales hemos buscado financiación fuera del marco de CTA a más de dos mil y dentro del marco de CTA o en cofinanciación a alrededor de mil. De ellos hemos financiado seiscientos noventa, que han supuesto casi quinientos diez millones de euros de ejecución, de los cuales ciento setenta millones han salido de nuestros fondos propios, que han supuesto la colaboración a modo de subcontratación con trescientos treinta y cinco grupos de investigación andaluces que han recibido por ello más de noventa millones de euros.

Por sectores, hay tres principales que copan prácticamente dos tercios de los proyectos que movilizamos en CTA: el sector Aeroespacial y Procesos Productivos (21%), el sector de Energía y Medio Ambiente (24%) y el sector de Tecnologías de Información y Comunicación (23%).

Algunas de las empresas de CTA son grandes empresas nacionales y multinacionales pero también tenemos empresas mucho más pequeñas, empresas basadas en conocimientos, empresas de base tecnológica e incluso *spin-off* universitarias. El apoyo es integral para todas ellas.

Nosotros consideramos que la fuerza de CTA es la fuerza de nuestra red, la capacidad de interconectar el ámbito privado con el ámbito empresarial y público, con las asociaciones de apoyo a la innovación y con los centros de generación de conocimiento.

CTA financia proyectos empresariales que tengan una duración inferior a tres años (queremos que sean proyectos que lleguen a mercado lo antes posible), que no se hayan iniciado, que se ejecuten mayoritariamente en Andalucía y que subcontraten grupos de investigación de manera que se produzca el proceso de transferencia del conocimiento. Al ser una entidad privada, además de financiar proyectos de I+D también tenemos la capacidad de financiar proyectos de innovación tecnológica a fondo perdido. También financiamos estudios de viabilidad (todo tipo de actividades previas a la ejecución de un proyecto), porque en algunas ocasiones creemos que es necesario ponerlos en marcha antes de abordar un proyecto largo y costoso de I+D+i que quizás no estaba bien definido de manera inicial y que podría acabar siendo un fracaso por no tener una planificación adecuada.

Nuestro proceso de evaluación es un proceso meritocrático. No le damos el mismo dinero a todos los proyectos sino que le damos más dinero al proyecto que consideramos que es mejor. Cuanto mejor sea la empresa, cuanto mejor haya planificado el proyecto y cuanto mejor defendido esté mayor garantía tendrá para su ejecución. Con esto no se pretende generar un filtro sino primar a quien tenga las ideas más claras, toda vez que creemos que será capaz de ejecutar un mejor proyecto.

La financiación, como también es en el caso del CDTI, es una financiación mixta, con una parte a fondo perdido y con una parte de crédito reembolsable (tres años de carencia y diez años de devolución). Queremos que los proyectos se ejecuten y sabemos que la liquidez es muy importante, por lo que damos un 50% por adelantado sin ningún tipo de aval. Y como queremos que los proyectos se pongan en marcha cuando se han de poner, nuestra convocatoria está siempre abierta hasta agotar fondos. Al ser privados, nuestros fondos son compatibles con otras financiaciones. No queremos ser un financiador principal de las actividades de las empresas sino ser una palanca de apoyo para la captación de fondos adicionales. Se trata de aprovechar los diferentes mecanismos de financiación de modo que con su unión generen una fortaleza mucho más potente que de manera individual.

Uno de nuestros proyectos históricos en el ámbito de la defensa fue el proyecto de detección a distancia de explosivos y residuos químicos y biológicos mediante una tecnología de espectrometría de plasma inducido por láser. Otro proyecto relevante fue uno con el que se pretendió conseguir que la fabricación aditiva pudiera ser un sustituto del almacenamiento de repuestos en situaciones complejas (como puede ser la propia de un submarino). Con un tercer proyecto, en esta ocasión de aplicación a las tecnologías de materiales, se trató de utilizar materiales compuestos avanzados para desarrollar alas integradas en aviones militares. Otro ejemplo de proyecto es un sistema de reconocimiento de personas en zonas de protección especial a través del iris, en tiempo real y en movimiento, esto es, sin necesidad obligar a las personas a colocarse delante de escáneres. Un último ejemplo, básicamente relacionado con el ámbito de la energía, es un proyecto mediante el cual se trató de desarrollar nuevos convertidores que fueran capaces de cumplir los requerimientos de energía y de potencia que necesitan los nuevos sistemas y nuevos programas de desarrollo militar (concretamente, los aviones F32 y F35).

Acrónimos y siglas

BRIEX	Brigada Experimental
C4I	Mando y Control, Comunicaciones, Computación e Inteligencia
CDTI	Centro para el Desarrollo Tecnológico Industrial
CIS	Sistemas de información y telecomunicaciones (*Communications and Information Systems)*
COINCIDENTE	Cooperación en Investigación Científica y Desarrollo en Tecnologías Estratégicas
DGAM	Dirección General de Armamento y Material
EDAP	Plan de acción europeo de la defensa (*European Defence Action Plan)*
EDF	Fondo europeo de defensa (*European Defence Fund*)
EDIDP	Programa europeo de desarrollo industrial en materia de defensa (*European Defence Industrial Development Program*)
ERC	Consejo europeo de investigación (*European Research Council*).
GAFA	Google, Apple, Facebook y Amazon
IED	Artefacto explosivo improvisado (*Improvised Explosive Device*)
IoT	Internet de las cosas (*Internet of Things)*
ISDEFE	Ingeniería de Sistemas para la Defensa de España
JCISAT	Jefatura de los Servicios de Información y Telecomunicaciones y Asistencia Técnica del Ejército de Tierra
MADOC	Mando de Adiestramiento y Doctrina
NBQ	Nuclear, Biológico y Químico
PADR	Acción preparatoria para la investigación en defensa (*Preparatory Action on Defence Research)*
PESCO	Cooperación permanente estructurada (*Permanent Structured Cooperation)*
PGE	Presupuestos Generales del Estado
RPAS	Aeronave pilotada remotamente (*Remotely Piloted Aircraft)*
STEM	Ciencia, tecnología, ingeniería y matemáticas (*Science, Technology Engineering and Mathematics)*
STO	Organización para la ciencia y la tecnología (*Science and Technology Organization)*