CENTRO SUPERIOR DE ESTUDIOS DE LA DEFENSA NACIONAL

DOCUMENTOS
DE SEGURIDAD Y DEFENSA

31

LAS NUEVAS TECNOLOGÍAS EN LA SEGURIDAD TRANSFRONTERIZA

MINISTERIO
DE DEFENSA

CENTRO SUPERIOR DE ESTUDIOS DE LA DEFENSA NACIONAL

LAS NUEVAS TECNOLOGÍAS EN LA SEGURIDAD TRANSFRONTERIZA

Febrero de 2010

MINISTERIO DE DEFENSA

CATÁLOGO GENERAL DE PUBLICACIONES OFICIALES
http://www.060.es

Edita:

MINISTERIO DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

NIPO: 076-10-063-8 (edición en papel)
ISBN: 978-84-9781-560-4
Depósito Legal: M-8091-2010
Imprime: Imprenta del Ministerio de Defensa
Tirada: 1.600 ejemplares
Fecha de edición: marzo 2010

NIPO: 076-10-064-3 (edición en línea)

Los autores quieren agradecer a don José Tomás González Partida, doctor ingeniero de Telecomunicaciones, sus aportaciones e información adicional suministrada para la confección de este Documento.

ÍNDICE

RESUMEN EJECUTIVO

El presente Documento *constituye el estudio que el grupo de trabajo sobre «Las nuevas tecnologías en la seguridad transfronteriza» ha realizado con el objetivo de analizar la problemática de la protección de las fronteras no reguladas en nuestro país y el problema de la autoprotección de nuestras Fuerzas Armadas en operaciones exteriores, desplegadas en territorio hostil o potencialmente hostil en un horizonte de los próximos 15-20 años.*

El Documento *se enmarca en los objetivos generales de la Comisión Permanente de Nuevas Tecnologías del Centro Superior de Estudios de la Defensa Nacional entre los que se encuentran el identificar y organizar grupos de expertos para realizar trabajos de análisis en las áreas científico-técnicas que se consideren más interesantes. Ha sido esta Comisión Permanente la que decidió constituir el grupo de trabajo responsable de la preparación del presente* Documento. *Éste está organizado en ocho apartados:*

- *Introducción y objetivos.*
- *El escenario global.*
- *Las amenazas para nuestra defensa y nuestra seguridad.*
- *Implicaciones en el desarrollo de las capacidades para combatir las futuras amenazas.*
- *Análisis de las tecnologías necesarias para el desarrollo de las* capacitades *relacionadas con la seguridad transfronteriza.*
- *Soluciones tecnológicas.*
- *Viabilidad del tejido tecnológico.*
- *Conclusiones.*

Introducción y objetivos

En este apartado se describe la constitución de la Comisión Permanente de Nuevas Tecnologías y se resume su propósito, para pasar a continuación a destacar la constitución del grupo de trabajo de «Las nuevas tecnologías en la seguridad transfronteriza» y a listar sus objetivos, orientados a analizar la problemática de la protección de las fronteras no reguladas en nuestro país y el problema de la autoprotección de la fuerza en operaciones desplegadas en territorio hostil. Análisis que deben conducir a contribuir a identificar las capacidades con que se habrían de dotar a las Fuerzas Armadas y a las Fuerzas y Cuerpos de Seguridad del Estado (FCSE) para hacer frente a la problemática con que se enfrentarán en un horizonte de los próximos 15-20 años.

El escenario global

Trata este apartado de conseguir definir que tipo de país tendremos y en que tipo de mundo estaremos en el horizonte de 15-20 años, para lo que se han definido cuatro escenarios posibles: gobierno global, multipolar, bienestar general y Occidente entre la amenaza y la atracción.

En la definición de escenarios, no hemos particularizado para España, sino que nos hemos centrado más en la Unión Europea. Tanto en lo concerniente a la propia problemática interna, como a las intervenciones exteriores en que se vea involucrada la Unión Europea y en donde España jugaría, previsiblemente un papel importante.

Se describe en detalle cada unos de los escenarios atendiendo a cinco variables dimensionales claves: la política global, la economía global, nuestro entorno europeo, nuestra casa y las amenazas y oportunidades que se identifican.

Dado que la situación actual global, de crisis financiera y económica nos aconsejaría no ser optimistas y centrarnos en los escenarios más pesimistas, el Documento *se ha orientado en principio a plantear soluciones tecnológicas para los escenarios más extremos con el lógico y humano deseo de que estemos equivocados y que el escenario futuro se aproxime más al de bienestar general.*

Las amenazas para nuestra defensa y nuestra seguridad

En este apartado se comienza con unas consideraciones previas que destacan la nueva visión de la defensa y la seguridad como necesidades interconectadas, frente a la visión clásica de separación entre seguridad como garantía de los derechos y libertades del ciudadano y defensa como protección de los intereses de la nación, que hacen que ambos conceptos hayan de ser tratados de forma integral.

Se pasa a continuación a la realización de un análisis del entorno estratégico que lleva asociada una evaluación de los riesgos y amenazas para desembocar en los escenarios de actuación de nuestras Fuerzas Armadas y de nuestras FCSE.

Todo ello con la finalidad de poder deducir implicaciones en el desarrollo y obtención de capacidades que permitan aprovechar de manera sinérgica las potencialidades tecnológicas españolas con las exigencias de nuestra seguridad nacional.

Implicaciones en el desarrollo de las capacidades para combatir las futuras amenazas

La evaluación de riesgos y amenazas realizada en el apartado anterior supone la extracción de una serie de implicaciones para el desarrollo de las capacidades adecuadas para el combate de las amenazas futuras.

Para conseguir el éxito en este combate, las Fuerzas Armadas y las FCSE deberán dotarse de unas capacidades que estén constituidas por la agrupación coherente de medios materiales, infraestructuras, recursos humanos, adiestramiento, doctrina de empleo y organización.

En el aspecto medios materiales, las tecnologías que se adopten (y adapten) para dotar a las Fuerzas Armadas y las FCSE deberán cumplir requisitos específicos en las facetas operativa, logística y de seguridad de su empleo tales como la consecución de la superioridad en el combate, de la interoperabilidad con aliados y facilitar la toma de decisiones.

La gestión integrada del apoyo logístico junto con la optimización de la formación, el empleo, la mentalidad y la motivación son aspectos a tener muy en cuenta en el diseño de la dotación de las capacidades.

El otro aspecto fundamental a considerar es el de las doctrinas. Éstas son a las organizaciones lo que la mentalidad a las personas, estructuran

la manera de pensar. Las doctrinas que las Fuerzas Armadas y las FCSE elaboren en el horizonte temporal que abarca este Documento *deberán estar más influidas por la incorporación de nuevas tecnologías que lo que lo vienen estando hasta el presente. Ello se deberá al hecho cada vez más evidente de que la tecnología transforma el entorno, porque lo hace con el tiempo y con el espacio, y además también nos trasforma a nosotros porque lo hace con nuestras dinámicas y con nuestras percepciones.*

Y por último, el aspecto de organización como componente importante del concepto capacidad ha de tenerse en consideración bajo la hipótesis posible, y deseable, que el aumento de información disponible desde los más bajos niveles hacia arriba evidencie la carencia de auténticos modelos de dirección estratégica de las organizaciones y motive su adaptación a esquemas más eficaces gracias a la ayuda de las tecnologías.

Análisis de las tecnologías necesarias para el desarrollo de las capacidades relacionadas con la seguridad transfronteriza

Este apartado se ha dedicado a revisar las tecnologías más directamente aplicables a la consecución de las capacidades de nuestras Fuerzas Armadas y las FCSE. Y el análisis se ha hecho tratando de proyectar la situación tecnológica actual al horizonte temporal que se plantea en este Documento.

Se han analizado los sensores, los vectores y las herramientas o tecnologías informáticas

Dentro de los sensores se han estudiado cuatro tipos: los sensores radar, los optrónicos, los enterrados tácticos y los receptores de análisis del espectro radioeléctrico.

Gran parte del éxito de los sensores analizados descritos depende de los vectores o plataformas usadas para desplegarlos. Es por ello que se han analizado tres tipos de plataformas apropiadas para embarcar sensores de vigilancia de fronteras: satélites, vehículos aéreos no tripulados y globos aerostáticos.

Y finalmente en el epígrafe «Herramientas informáticas», p.68 aplicables a la consecución de las capacidades, se han analizado las tecnologías siguientes: Arquitecturas Orientadas al Servicio (SOA), lenguajes de programación, sistemas operativos, herramientas de desarrollo, Sistemas

de Presentación Geoespacial Avanzada, Sistemas Expertos de Búsqueda (Data Mining) *y Sistemas de Tratamiento y Proceso de Imágenes.*

Soluciones tecnologías

Como se deduce de los apartados anteriores, el estado actual y futuro de la tecnología ofrece un amplio abanico de soluciones parciales a la problemática de la protección de las fronteras no reguladas en nuestro país y al problema de la autoprotección de la fuerza en operaciones desplegadas en territorio hostil. Diversos tipos de sensores operados desde plataformas también diferentes pueden ofrecer a los operadores de los sistemas varias visiones, distintas e incompletas, del escenario fronterizo. Dar una solución tecnológica global al problema en un entorno geográfico concreto implica necesariamente la integración de distintos sistemas, procesando la información provinente de diferentes sensores de forma que también se aprovechen las mejores características de cada uno de ellos.

En este apartado se ha analizado la utilización del concepto sistémico NEC (Network Enabled Capability) *que responde a la necesidad de disponer de sensores y de sistemas de apoyo al mando y unidades de respuesta a las amenazas, interconectados de manera que se aproveche de forma adecuada toda la información disponible, traduciéndose en una mejor y más eficiente actuación por parte de los agentes implicados. La base fundamental sobre la que se sustenta este nuevo concepto, reside en el valor de la información y la superioridad que se puede obtener al disponer de información precisa y relevante en el momento oportuno. Como medio para lograr dicha superioridad, se plantea la conexión en una red común a todas las entidades de interés, que participan de algún modo en las operaciones, de forma que cada elemento usuario pueda generar, conocer, aprovechar y difundir la información que pueda resultar útil en cada instante.*

Someramente, debido a las limitaciones de espacio, se han analizado también en este apartado las diferentes tecnologías aplicables a la implantación del concepto NEC, deteniéndose especialmente en el de SOA y finalmente se ha hecho un ejercicio específico de un modelo de sistema que utiliza las arquitecturas tecnológicas descritas como ejemplo demostrativo de cómo se puede abordar una solución de siste-

ma aplicable a la consecución de las capacidades de nuestras Fuerzas Armadas y las FCSE.

Viabilidad del tejido tecnológico

Dado que el objetivo de este trabajo es el hacer un ejercicio de cómo se deberían dotar nuestras Fuerzas Armadas y FCSE ante las amenazas que se predicen en los escenarios futuros de un horizonte de 15-20 años, en el grupo de trabajo, se ha considerado importante completar el Documento *con un breve análisis de la problemática del tejido tecnológico español en cuanto a su grado de adaptación para que nuestro país pueda conseguir una superioridad tecnológica futura cara a las amenazas que se describen en este* Documento. *Este análisis incide en como los diferentes grupos de interés del tejido industrial tecnológico español deberían de coordinarse con la universidad y con los responsables operativos de las Fuerzas Armadas y de las FCSE para conseguir una base tecnológica integrada capaz de dar respuesta al objetivo de superioridad tecnológica que se plantea.*

INTRODUCCIÓN Y OBJETIVOS

La Comisión Permanente de Nuevas Tecnologías está constituida por un conjunto de expertos en tecnología y defensa, encargado, en el nivel académico, de estudiar, proponer y ejecutar, en su caso, el desarrollo de planes tecnológicos a corto y medio plazo compartido por la universidad, la industria, las Fuerzas Armadas y las Fuerzas y Cuerpos de Seguridad del Estado (FCSE).

Esta Comisión tiene, entre otros los siguientes objetivos generales:

- Editar un catálogo de necesidades tecnológicas de las Fuerzas Armadas y de las FCSE.
- Editar un catálogo de capacidades tecnológicas a cargo de la universidad y de la industria del sector.
- Facilitar la colaboración entre universidad, industria, Fuerzas Armadas y FCSE en el ámbito de la investigación tecnológica.
- Identificar y organizar grupos de expertos para realizar trabajos de análisis en las áreas científico-técnicas que se consideren más interesantes.

La Comisión, desde la constitución de su acta fundacional, ha impulsado la creación de varios grupos de trabajo, entre los que se encuentran el de «Las nuevas tecnologías en la seguridad transfronteriza», que comenzó su actividad en octubre del año 2008, y que está constituido por miembros de los cuatro estamentos: universidad, industria, las Fuerzas Armadas y las FCSE.

Los objetivos que se ha marcado también en este grupo de trabajo, son los siguientes:

– Analizar la problemática de la protección de las fronteras no reguladas en nuestro país.
– Analizar el problema de la autoprotección de la fuerza en operaciones desplegadas en territorio hostil o potencialmente hostil.
– En un horizonte cercano: los próximos 15-20 años.
– Contribuir a identificar las capacidades con que se habrían de dotar las Fuerzas Armadas y las FCSE para hacer frente a la problemática identificada.

Como país miembro de la Unión Europea y por nuestra posición geográfica, somos garantes de la impermeabilización de nuestras fronteras marítimas, que resultan fronteras exteriores de la Unión Europea. La parte de estas fronteras de naturaleza no regulada ya están siendo tratadas por España a través del Programa SIVE del Ministerio del Interior. Sin embargo, la problemática conocida de las amenazas de inmigración ilegal que procede de las costas africanas lejanas del Atlántico Sur: Mauritania, Senegal y Cabo Verde está aún pendiente de resolverse de una manera competitiva en la relación coste-eficacia. Es pues esta una problemática a analizar, junto con la mejora de las prestaciones del actual Programa SIVE y el tratamiento de futuras amenazas que actualmente no se contemplan (aeronaves de baja cota y ataques terroristas con vehículos controlados remotamente).

Entendemos que es objetivo de este grupo de trabajo el analizar el problema de la autoprotección de la fuerza en operaciones desplegadas en territorio hostil o potencialmente hostil y es por ello que ha sido identificado como tal.

El objetivo anterior implica utilizar técnicas de vigilancia perimetral cercana y medidas similares a las que se puedan utilizar en la impermeabilización de fronteras terrestres no reguladas.

Y finalmente se reconoce también como objetivo de este grupo de trabajo el contribuir a identificar las capacidades con que se habrían de dotar las Fuerzas Armadas y las FCSE para hacer frente a la problemática analizada. Utilizamos el concepto «capacidades» siguiendo la metodología: cómo está organizado, cuales son sus miembros y qué plan de trabajo se ha planteado para conseguir los objetivos enunciados.

En resumen, desde el grupo de trabajo de «Las nuevas tecnologías en la seguridad transfronteriza» se ha pretendido contribuir a mejorar la sinergia necesaria entre los pilares investigador y productivo y el cliente y usuario de la tecnología para afrontar exitosamente los retos de seguridad y defensa de España y fortalecer el tejido industrial e investigador de nuestro país.

EL ESCENARIO GLOBAL

En este capítulo se trata de conseguir definir lo siguiente:

> «Que tipo de país tendremos y en que tipo de mundo estaremos en *el horizonte de 20-25 años.*»

Para ello se han definido cuatro escenarios posibles:

1. Gobierno global
2. Multipolar.
3. Bienestar general.
4. Occidente entre la amenaza y la atracción.

Describiremos cada escenario atendiendo a unas variables dimensionales que se consideradas claves:

– La política global.
– La economía global.
– Nuestro entorno europeo.
– Nuestra casa.
– Las amenazas y oportunidades que se identifican.

En la definición de escenarios, no hemos particularizado para España, sino que nos hemos centrado más en la Unión Europea ya que al ser Estado miembro importante de la Unión Europea, y contar con fronteras exteriores hacia una vecindad problemática, se puede constatar que los conflictos, problemas y oportunidades que se describen en los diferentes escenarios, son perfectamente aplicables a nuestro país. Tanto en lo concerniente a la propia problemática interna, como a las intervenciones exteriores en que se

vea involucrada la Unión Europea y en donde España jugaría, previsiblemente un papel importante.

La situación actual global, de crisis financiera y económica nos aconsejaría no ser optimistas y centrarnos en los escenarios más pesimistas, que son precisamente los más demandantes de políticas exigentes de seguridad en las que la tecnología juegue un papel importante. Es por ello que este *Documento* se ha orientado en principio a plantear soluciones tecnológicas para los escenarios más extremos con el lógico y humano deseo de que estemos equivocados y que el escenario futuro se aproxime más al de bienestar general.

Pasamos también a continuación a describir los diferentes escenarios analizados.

Escenario de gobierno global

Se trata de un mundo futuro en donde los problemas globales, en particular el cambio climático, inducen a las potencias mundiales a embarcarse en una estrategia sin precedentes de cooperación de largo alcance. Durante una o dos décadas la confianza y el entendimiento global crecen de forma sólo recordada en los años de inicio de la integración europea y Europa es vista como un modelo para esta nueva integración mundial.

De forma global, se ponen en marcha proyectos, que pretenden ser eficaces, para mitigar y adatarse al cambio climático, así como programas de desarrollo masivo en las regiones desfavorecidas. Estas inversiones a gran escala en combinación con un comercio mundial progresivamente más abierto conducen a la economía mundial a un largo periodo de gran crecimiento en el que China juega un papel creciente.

Los programas de desarrollo en las regiones más desfavorecidas incluyen también a la globalidad de los países vecinos de la Unión Europea.

En Europa la explosión del crecimiento económico beneficia no sólo a las economías regionales más preparadas y basadas en el conocimiento, sino también a los grupos marginales étnicos de los barrios periféricos urbanos y a su joven población. Sin embargo, no todas las capas de la sociedad europea disfrutan de un desarrollo positivo. Algunas regiones con población e infraestructura productiva envejecida tienen problemas para enfrentarse a la competencia global y ello provoca resentimientos que acaban radicalizando la política con sentimientos xenófobos.

Sin embargo, se producen tendencias centrífugas entre todo el conjunto de Estados miembros, debido a las diferencias de adaptación de algunos de ellos a la nueva situación de explosión económica global.

China supone una fuerte influencia tanto en lo económico como en lo político y en lo cultural. Mientras que la sociedad china llega a una cierta liberalización debido a la intensificación de los contactos con Europa y Estados Unidos, se produce un efecto contrario: muchos occidentales quedan impresionados por la eficacia y eficiencia china, basada en el respeto confuciano a la autoridad y se produce un descenso en Europa, en la aceptación de comportamientos antisociales.

Un aspecto de estos cambios de valores es un deseo y una aceptación creciente de medidas de seguridad que invadan la intimidad y que impliquen pérdida de tiempo. Aparece una apetencia general de soluciones de colaboración entre lo público y lo privado en el ámbito del sector de seguridad. Además de actores comerciales, como empresas de vigilancia y seguridad, empiezan a tener un papel importante organizaciones de voluntarios (ciudadanos por la seguridad).

En este escenario se identifican también dos problemas relacionados con la seguridad:

– Una Europa de dos velocidades que también puede favorecer el crimen organizado.
– Poco interés de la ciudadanía en invertir en seguridad.

Escenario multipolar

En este escenario tenemos un mundo futuro caracterizado por la competencia y la falta de confianza entre las potencias mundiales líderes: China, India, Japón, Unión Europea y Estados Unidos. Por consiguiente no se acuerdan políticas globales para luchar contra el cambio climático ni para conseguir mitigarlo o adaptarse al mismo.

El crecimiento económico global se ralentiza o para la causa de los efectos que produce el cambio climático y a la tendencia al manejo del comercio, sin llegar a la autarquía, dentro de cada potencia y de sus territorios de influencia.

Los efectos negativos del cambio climático comienzan a declararse, aunque de manera menor en la Unión Europea y su vecindad, agravando los problemas ya existentes de escasez de agua y alimentos. Estas condicio-

nes se mezclan con una competencia desmedida en la búsqueda de recursos energéticos y minerales, que conducen a conflictos étnicos y guerras tribales.

Mientras que la cohesión europea es fuerte a nivel estatal, el conflicto social es endémico. Se produce una radicalización violenta entre dos capas sociales opuestas y fuertemente impactadas por una economía débil: la clase trabajadora blanca y la clase media acomodada, frente a los suburbios de segregación étnica con su mezcla de tercera y cuarta generación de emigrantes y los refugiados recientes llegados como consecuencia de las catástrofes sociales y medioambientales que se están produciendo.

En este peligroso entorno de graves conflictos se aceptan medidas de seguridad agresivas e invasoras de la privacidad. De forma general, la seguridad se ve como una responsabilidad de los gobiernos, lo que significa, por ejemplo, que algunas actividades que anteriormente se subcontrataban a empresas privadas de seguridad se vuelven a ejecutar internamente por organizaciones gubernamentales. El sector de la seguridad apuesta por un fuerte desarrollo al más puro estilo militar de la guerra fría con programas a gran escala liderados por las empresas más grandes.

En este escenario se identifican varios problemas:

- Intervenciones en eventos del tipo crisis humanitarias en regiones inestables de la Tierra (por ejemplo Bangladesh), tendrían que ser realizadas solamente por la Unión Europea y sin el apoyo logístico de Estados Unidos. Ello debido al hecho de que los deseos de cooperar por parte de otras potencias mundiales serían limitados en este escenario. La Unión Europea debería dotarse entonces de mejores capacidades para poder conducir intervenciones a gran escala con toda clase de medios.
- Más crimen organizado como derivada de las guerras tribales y los conflictos étnicos.
- Inestabilidad financiera y competencia entre monedas.
- Presiones migratorias que consolidan también la mentalidad de Europa como fortaleza a alcanzar.
- Aumento de los secuestros.
- Aumento de la violencia en los suburbios.
- Ataques a infraestructuras de la Unión Europea en el exterior.
- Espionaje industrial.
- Proliferación de tecnologías incontroladas debido a la falta de cooperación entre las potencias mundiales.

Escenario de bienestar general

En este mundo futuro Estados Unidos y sus aliados vuelven a conseguir el compromiso de los años noventa de promover la democracia liberal y los derechos humanos a lo largo y ancho del Planeta con una combinación de uso blando y duro del poder, pero con preferencia por el primero. La posición de defensa de los derechos humanos implica que las relaciones con las autoritarias China y Rusia sean relativamente tirantes. La Unión Europea y Estados Unidos ponen en marcha políticas para mitigar el cambio climático aunque con una eficacia limitada debido a una falta de compromiso del resto del mundo. Ello debilita la legitimidad y el acuerdo de invertir en políticas de cambio climático.

La economía crece de forma sostenida y equilibrada a largo plazo. Aunque se entra en una nueva era de cambios estructurales en el que se desarrollan Pequeñas y Medianas Empresas (PYMES) innovadoras que juegan un papel importante en la industria.

En África y en Oriente Medio se produce un desarrollo social positivo. Sin embargo, el impacto ambiental que causa el cambio climático es elevado, lo que produce un aumento de la presión migratoria hacia Europa provocado por estas razones ambientales y sus consecuencias económicas.

La cohesión europea es fuerte, tanto a nivel de Estados miembros como de los estratos sociales. La cooperación entre el sector público y el privado produce efectos beneficiosos en el sector industrial generando PYMES altamente innovadoras que se transforman en el motor del bienestar para todos. Este ambiente de desarrollo político y social positivo en la Unión Europea se extiende a su vecindad ayudando a corregir los desequilibrios del inicio del siglo XXI.

El gran énfasis en los derechos humanos pone límites estrictos a las medidas de seguridad. Entre estos límites destaca la tendencia a la externalización y al desarrollo de soluciones innovadoras que desde el sector privado se transfieren a la seguridad. Se ponen en marcha nuevas medidas políticas para promover y explotar servicios y soluciones innovadoras.

Aspectos destacados del escenario:

- Poco interés en invertir en seguridad.
- Poca aceptación de medidas de seguridad.

Escenario Occidente entre la amenaza y la atracción

Es un mundo futuro caracterizado por estar sumergido en una lucha continua contra el terrorismo extremista. Son Estados Unidos inicialmente y una Unión Europea como compañero júnior, los que soportan las consecuencias de este escenario. Una consecuencia de este escenario, se produce en las áreas vecinas de la Unión Europea donde se desarrollan conflictos armados de diversos tipos. En relación con los otros actores mundiales principales (en particular China y Rusia), Estados Unidos y por tanto la Unión Europea, mantienen una postura diplomática de cooperación en asuntos de interés mutuo. En concreto, el yihadismo militante es un problema para todos. Sin embargo, estos intentos de cooperación no implican el compartir los mismos valores lo que produce una falta de confianza continua entre sus miembros. En casos de interés unilateral, se hace muy difícil conseguir el soporte de los otros.

La situación de conflicto global deja escasos recursos a la lucha contra el cambio climático, aunque se aprecie un impacto negativo creciente consecuencia del mismo.

No obstante el crecimiento económico a largo plazo mantiene una tasa moderada. Es un periodo de estabilidad estructural dominado por grandes empresas tradicionales empeñadas en conseguir economías de escala por medio de adquisiciones y fusiones al tiempo que externalizan la producción y los servicios con bajo valor añadido. La falta de confianza general en el futuro, resultado de incertidumbres en el suministro de materias primas y en el riesgo de conflictos políticos, limita la explotación del potencial económico. El comercio y las inversiones, incluso en nuevas tecnologías, tienden a estancarse a pesar de la aparición de nuevas oportunidades emergentes en América Latina y, aunque muy lentamente en África.

En las áreas vecinas de la Unión Europea, los conflictos políticos, sociales y religiosos, se ven agravados por las crisis medioambientales. En suma, la Unión Europea se enfrenta a un crecimiento de la presión migratoria.

Además, el conflicto produce sentimientos negativos entre algunos de los ciudadanos y otros habitantes con conexiones étnicas o ideológicas con las zonas de conflicto principales.

Al mismo tiempo, la realidad de la amenaza terrorista fuerza a los Estados miembros de la Unión Europea a desarrollar y cumplir con estrategias y políticas de seguridad con una proyección de largo alcance que garanticen la cohesión en la lucha con conflicto constante. Asimismo, en vista de la

magnitud de las amenazas en el horizonte y de los costes asociados para combatirlas, las responsabilidades en áreas clave de política de seguridad y en su implantación (por ejemplo, seguridad de fronteras tanto en términos de flujos de inmigración como de producción de tecnología) se trasladan al nivel comunitario europeo.

En este peligroso escenario de conflictos se aceptan medidas de seguridad de largo alcance que a su vez invaden la privacidad ciudadana. Las operaciones de seguridad se subcontratan en un grado considerable a firmas comerciales.

Aspectos a destacar

En general, la problemática de este escenario es bastante pronunciada. Se caracteriza por una extrema diversidad de variables y de requisitos cara a la definición de políticas de seguridad. Ello implica que las medidas necesarias y los costes y esfuerzos asociados son inevitablemente altos. Al ser la seguridad un aspecto de máxima prioridad en las agendas políticas, hay una gran predisposición a dedicar recursos suficientes en este apartado. Y con el objeto de aumentar la eficacia de las medidas y las políticas de seguridad, las responsabilidades se centralizan y se refuerzan políticas más estrechas de cooperación a nivel transnacional. No obstante, no está claro si la Unión Europea tendrá capacidades y recursos suficientes para enfrentarse con las amenazas:

1. La fase actual de globalización ha llevado a una situación de dependencia económica mutua en servicios clave que se están proporcionando desde cualquier lugar. Esto incluye la provisión de servicios de infraestructura (sistemas de atención, *software*, producción, etc.) sin los que nuestro sistema económico no puede operar. A pesar de los esfuerzos para evitar las localizaciones de mayor conflictividad, el riesgo creciente de conflictos locales lleva repetidamente a la interrupción de la provisión de servicios de la tecnología de la información básicos:
   – Este tipo de riesgo lleva a repensar las condiciones del marco económico para la subcontratación de servicios y de producción y los esfuerzos para asegurar la provisión de actividades domésticas clave. Este tipo de proteccionismo no está motivado por razones económicas sino por preocupaciones de seguridad.

2. En este escenario se dan frecuentemente conflictos locales. Son atendidos mediante misiones especiales de seguridad que se parecen mucho a las intervenciones convencionales armadas militares, pero que están dirigidas a controlar la situación conflictiva. En estas situaciones, las acciones de seguridad militar y civil convergen y se integran transformándose en una especialidad europea:
   – Estos conflictos locales pueden ser incluso de naturaleza nuclear (India-Pakistán).
   – La proliferación de armas de destrucción masiva pasa a ser un punto de gran importancia.
   – Las tecnologías que aseguren una buena calidad de alerta de la situación global, tales como vigilancia satelital, serán utilizadas para apoyar las intervenciones.
   – Se demandará protección civil y medidas preparatorias para flujos crecientes de refugiados y de emigrantes hacia Europa en las áreas de conflicto local.
3. La situación de conflicto global con varios conflictos locales emergentes inducirá un aumento importante en los costes de los recursos, variando desde agua a petróleo y otros. El tema agua será particularmente importante desde una perspectiva europea si se concibe una ampliación en el año 2030, en donde se incluya por ejemplo Turquía y otros países con problemas serios de suministro de agua. Se harán esfuerzos importantes para aumentar la eficacia de los recursos, su uso y reciclado, pero esto no será suficiente para contrarrestar completamente los futuros periodos de escasez:
   – Como consecuencia de esta situación, se verá un renovado y aumentado interés en el uso de la energía nuclear, al menos aquellos países que tienen acceso a la tecnología apropiada y a los recursos naturales que aseguren el suministro de combustible nuclear. Ello por su parte mejorará los riesgos asociados con la proliferación de esta tecnología nuclear.
   – La seguridad en el suministro de recursos naturales importantes estará haciendo crecer las intervenciones políticas y militares para garantizar los intereses económicos y también el acceso a los recursos clave.
4. Los conflictos locales y regionales pueden aumentar la presión en las fronteras europeas en un factor de cinco a diez en comparación con

la actualidad. Mientras el flujo de emigrantes pueda resultar positivo en muchos aspectos, el deslizamiento demográfico producido en Europa, hace crecer la diversidad de la sociedad europea y conlleva a la emergencia de nichos de comunidades hostiles a la Unión Europea dentro de nuestras fronteras. Se introducen mejores tecnologías para vigilar y controlar las fronteras junto con seguridad urbana como respuesta a leyes más estrictas:

- Reconociendo la ambivalencia y al mismo tiempo inevitable carácter del crecimiento de la inmigración, tanto la legal como la ilegal, se requiere realizar esfuerzos para controlar esta inmigración.
- Es probable que este escenario requiera una aproximación europea más integrada en seguridad de fronteras, debido a los requisitos financieros y técnicos más elevados que los países aisladamente no podrían soportar. La tendencia general integradora en materias de seguridad en este escenario nos conduce a esa necesidad.
- Alrededor del año 2030, las amenazas desde el espacio aéreo serán más serias para la seguridad que 15 años antes.
- Las armas de destrucción masiva se transformarán en una de las amenazas principales en el año 2030 obligando a un esfuerzo en la detección temprana de ellas.
- Se espera que aparezcan nuevos conflictos sociales en las ciudades europeas debido a la falta de estabilidad social, a la segregación racial y al aumento de las diferencias sociales.

5. Las crisis humanitarias son más frecuentes, tanto en la vecindad de la Unión Europea (fronteras de Ceuta y Melilla) como a grandes distancias (*tsunami* en Indonesia). Estas crisis están asociadas a las situaciones de conflicto, pero también originadas por desastres naturales como consecuencia del cambio climático. Las capacidades para la intervención en tales situaciones de crisis humanitarias necesitarán ser por tanto aumentada y mejorada.
6. El crimen organizado con fuente en Rusia, Asia y en los Balcanes, será un problema serio. Es difícil de combatir debido a la falta de apoyo por parte de los países del origen del mismo.

LAS AMENAZAS PARA NUESTRA DEFENSA Y NUESTRA SEGURIDAD

Es muy probable que el escenario mundial a medio y largo plazo sea reconocible en alguno de los escenarios descritos anteriormente (recordemos, «gobierno global»; «multipolar», «bienestar general» y «Occidente entre la amenaza y la atracción») o en una combinación de los mismos.

Es cierto que uno de ellos predominará sobre el resto, pero la tensión entre unos y otros será la que vaya vertebrando la Historia, de manera que en cada momento podremos reconocer rasgos característicos de cada modelo, rasgos que se irán combinando, alternando y sucediendo en el tiempo y el espacio.

Sin embargo, no es realista asumir que la seguridad y la defensa de España y de nuestro entorno europeo, al que como se ha mencionado anteriormente, estamos indisolublemente vinculados, van a dejar a estar amenazadas.

Se trata pues de identificar una serie de denominadores comunes que, asumidos, nos permitan estar preparados para el más exigente de los escenarios sin descartar que puedan, deseablemente, llegar a ser innecesarios.

Por lo tanto, a continuación se propone una particularización de los escenarios descritos anteriormente para nuestro ámbito más próximo, España y la Unión Europea.

Defensa y seguridad como necesidades interconectadas

La separación clásica entre seguridad como garantía de los derechos y libertades del ciudadano y defensa como protección de los intereses de

la nación ya no traduce la realidad del complejo escenario estratégico del primer cuarto del siglo XXI.

Hoy, y a corto y medio plazo esta tendencia tiene visos de consolidarse, el límite entre las amenazas asociadas a la delincuencia y las amenazas asociadas a actores nacionales agresivos o conflictivos se va difuminando. La consecuencia debe ser que lo que nos protege de una y otra va tomando la forma de un sistema integrado de seguridad nacional cuyos recursos deben estar forzosamente coordinados.

Esto no quiere decir que sea necesaria una amalgama de organizaciones ni una reestructuración de las instituciones encargadas de proveer seguridad a la nación, sino que su funcionamiento debe ser sinérgico en general y en los campos donde su actuación se solapa, cuidadosamente armonizada.

A este estado de cosas nunca ha sido ajena la investigación ni la industria. El resultado es que su producto, la tecnología, es un hecho neutro de por sí. La tecnología, independientemente de su origen, no está marcada de antemano. Al contrario, se trata de una especie de materia prima que la imaginación y el acierto de sus gestores puede convertir en un multiplicador de capacidades y la herramienta definitiva para resolver los problemas que, como hemos visto, están cada vez más interconectados en el campo de la seguridad y la defensa.

Por lo tanto, si ya de manera conceptual la seguridad y la defensa conforman un continuo que hay que gestionar integralmente, las tecnologías subyacen a ese continuo formando la capa sobre la cual se asientan los sistemas.

El trasvase de tecnologías es un fenómeno consustancial a la imaginación del hombre. Desde la invención de la pólvora por alquimistas chinos a la aplicación médica de los avances en la carrera espacial la Historia está llena de ejemplos.

La adaptación a otros campos de tecnologías que originariamente han surgido y se han generalizado en España como respuesta a la necesidad de controlar el fenómeno de la inmigración masiva e ilegal es cuestión de tiempo y de acierto de los responsables.

Pero, ¿cuáles son estos campos? los párrafos siguientes constituyen un recorrido que partiendo del análisis del entorno estratégico, pasa por una evaluación de riesgos y amenazas para desembocar en la descripción de los escenarios de actuación más probables de nuestras Fuerzas Armadas y nuestras Fuerzas y Cuerpos de Seguridad del Estado (FCSE). Todo ello con la finalidad de poder deducir implicaciones en el desarrollo y obtención

de capacidades que permitan aprovechar de manera sinérgica las potencialidades tecnológicas españolas con las exigencias de nuestra seguridad nacional.

Entorno estratégico

Sin contradecir el enfoque anterior sobre la interconexión de las necesidades de seguridad y defensa, es evidente que la descripción de un entorno estratégico debe diferenciar condicionantes generales, aquellos que afectan a la actuación clásica de la Fuerzas Armadas y las que pudieran afrontar en el medio y largo plazo las FCSE.

Así, con respecto a las condiciones generales del entorno estratégico cabe destacar:

- En el corto y quizá medio plazo el factor más novedoso y de calado en el escenario internacional es la crisis económica. Su alcance mundial afectará a los gobiernos y a su capacidad de inversión en tecnologías sin que ello impida a actores agresivos poder disponer de ellas. En este contexto de crisis económica, la aplicación de tecnologías polivalentes debe ser la base para mantener la superioridad requerida.
- La situación estratégica actual se caracteriza por una acelerada velocidad de cambio, consecuencia del fenómeno de la globalización. Las posibilidades de interacción entre los diferentes grupos humanos aumentan y a su vez incrementan la probabilidad de conflicto, con unos riesgos y amenazas que cada vez son más complejos e interrelacionados. En el medio plazo esta tendencia se consolidará. Los intercambios generan la aparición de intereses y en el choque de éstos se encuentra el germen de los conflictos.
- En estrecha relación con el factor económico mencionado anteriormente se encuentra la competencia por los recursos energéticos, que marcará las próximas décadas de las relaciones internacionales. Lo que normalmente se venía vehiculando a través de los mecanismos del mercado, en momentos de crisis o escasez puede llegar a convertirse en generador de conflictos.
- La aparición de un esquema espacio-tiempo virtual materializado en la Red, abre una nueva dimensión de la seguridad. Las redes in-

formáticas se convertirán en los «campos de batalla» y las «escenas del crimen» de la próxima generación, sin descartar las tradicionales, desgraciadamente.

En el campo estricto de los conflictos armados, el ambiente en el que se desarrollarán participará sin duda de las siguientes características:

– La globalización ha permitido que grupos no estatales sean capaces de actuar e influir sustancialmente en el escenario internacional. Sin que se prevea una eclosión descontrolada de este tipo de agentes, habrá que contar con ellos en el número y potencia que permitan las economías de escala.
– El abaratamiento y disponibilidad generalizada de las tecnologías más avanzadas no sólo mejoran sustancialmente las capacidades de las Fuerzas Armadas sino que también proporcionan a nuestros posibles oponentes el acceso a un escenario global. Por lo tanto, en el futuro inmediato y a medio plazo el empleo de estrategias asimétricas se convertirá en lo habitual.
– Aunque la posibilidad de conflictos generalizados de corte convencional entre Estados y coaliciones es baja, no puede descartarse. Un punto en el globo terráqueo que atrae poderosamente la mirada cuando barajamos esta posibilidad es el Oriente Próximo. La proliferación de armas de destrucción masiva unida a la obtención de capacidades de proyección, obligan a prever conflictos de una naturaleza más convencional siquiera desde el punto de vista de los actores participantes.
– Las organizaciones internacionales y de defensa colectiva continuarán participando en operaciones de apoyo a la paz dentro de un contexto de promoción de la seguridad y estabilidad mundiales. La participación de nuestras Fuerzas Armadas en operaciones de este tipo debe darse por segura, en uno u otro formato y con mayor o menor intensidad, en las próximas décadas.

Siguiendo este esquema, el entorno que a medio y largo plazo puede afectar al trabajo y las responsabilidades de las FCSE puede quedar descrito como sigue:

– Las presiones ejercidas por la modernización, la crisis cultural, social y política, y la enajenación de los jóvenes que viven en sociedades extranjeras finalizarán con frecuencia en alguna modalidad

de terrorismo. Resultando indispensable una actuación europea concertada para su lucha por parte de las FCSE.

– Un factor influyente en la seguridad será el continuo crecimiento de población inmigrante, debiendo adaptarse las FCSE a este movimiento para evitar las posibles consecuencias de falta de adaptación social, problemas de identidad cultural, frustración ocasionada por el incumplimiento de sus expectativas individuales o familiares, etc. Llegando éstos a integrarse en organizaciones delictivas o al extremismo religioso que finalice en terrorismo.
– Debido a la crisis económica y al desequilibrio que se crea entre naciones. Habrá que tener muy en cuenta la delincuencia organizada como el tráfico de drogas, la trata de seres humanos o el tráfico de armas, los cuales no se detienen en la frontera de una nación. La delincuencia organizada puede tener vínculos con el terrorismo y, en casos extremos, puede incluso llegar a dominar al Estado.
– La mala gestión de los asuntos públicos (corrupción, abuso de poder, debilidad de las instituciones e incumplimiento de la obligación de rendir cuentas) y los conflictos civiles corroen a los Estados desde dentro. Esta situación puede conducir al hundimiento de las instituciones oficiales: el Afganistán de los talibanes es un ejemplo conocido.
– La falta de cohesión social limita la capacidad ejecutiva de los gobiernos en los ámbitos de política exterior y seguridad. La existencia, dentro de un Estado, de grupos de presión de carácter económico, social, cultural, religioso o étnico puede perjudicar o condicionar la toma de decisiones, tanto en política interior como exterior. Siendo esto probable en la sociedad multicultural y plural en la que vivimos.
– Hay que tener en cuenta, que desde finales del siglo XX se está produciendo un notable renacimiento religioso a nivel mundial. En la mayoría de las religiones han surgido movimientos fundamentalistas, algunos de los cuales tienen en determinados países un alto poder de influencia política, que preconizan la pureza de las doctrinas y promueven una modificación de las conductas personales, sociales y públicas.
– El avance tecnológico que vivimos al igual que las Fuerzas Armadas, permite a las FCSE incrementar sus medios de lucha en las labores de seguridad, pero las organizaciones delictivas y los te-

rroristas también avanzan en este sentido, provocando una carrera continua en la que siempre debemos ir por delante para evitar sus acciones.

– De manera análoga a las Fuerzas Armadas, las FCSE participarán en las operaciones de paz como: observación de los acuerdos de paz o de los derechos humanos, en labores de policía con misiones ejecutivas, en asistencia técnica, como fortalecimiento institucional o *training* como fase de un proceso de paz.
– Resulta significativo comprobar que, durante los días posteriores a los ataques terroristas del 11 de septiembre de 2001 en Nueva York, los de Casablanca en mayo del 2003 y más recientemente los sufridos en Madrid el 11 de marzo de 2004, los flujos migratorios en pateras que habitualmente transitan desde Marruecos a España cesaron completamente, cuando normalmente se producen numerosos desplazamientos diarios. Dada la escasa estructura en interrelación de las diferentes redes de tráfico de personas que operan en Marruecos, este hecho parece demostrar la existencia de un poder coercitivo que, si bien no puede suprimir el fenómeno en su totalidad, tiene capacidad para reducirlo a niveles muy inferiores a los actuales.

Riesgos y amenazas

¿Cómo se traduce este entorno estratégico, general y de horizonte temporal amplio en un análisis de riesgos y amenazas tangibles?

Los riesgos, esto es, las actividades o factores de peligro que no están absolutamente bajo control, y las amenazas, que implican una voluntad contraria, se pueden agrupar en:

– Agresiones contra el territorio nacional o la violación de los espacios de soberanía.
– La proliferación de armas de destrucción masiva.
– El terrorismo como estrategia de actuación y también de influencia política.
– Los ataques cibernéticos y contra los sistemas de telecomunicaciones e información que pueden llegar a colapsar la vida de la nación o poner en peligro información sensible.

– La interrupción de las líneas de suministros de recursos básicos, principalmente los energéticos
– El crimen organizado, incluyendo entre otros la piratería y el tráfico de armas y drogas.
– La inmigración ilegal, y el tráfico de seres humanos.
– Las catástrofes naturales, de origen humano o natural.

De todos ellos, se sigue considerando el terrorismo como la principal amenaza en un futuro inmediato. La posibilidad de que los grupos terroristas de carácter transnacional tuvieran acceso a las armas de destrucción masiva representa, por otro lado, la hipótesis más peligrosa.

Además, se han identificado una serie aceleradores capaces de acortar los tiempos para que esos riesgos se conviertan en realidades:

– La globalización, que facilita la interconexión de amenazas. Este fenómeno implica también una mayor difusión del conocimiento, lo que puede facilitar el acceso a la tecnología militar y a nuevas tendencias y desarrollos militares.
– La crisis financiera, que generaliza los estados de disconformidad y de precariedad. A su vez, ésta puede ser utilizada como excusa para favorecer la radicalización ideológica, justificando de esta forma comportamientos agresivos por parte de determinados actores, o bien usarse esos comportamientos agresivos como forma de desviar la atención respecto a los problemas internos. Todo ello, finalmente, puede repercutir en un aumento de la conflictividad.
– La proliferación de instalaciones nucleares, incluso con uso civil, en Estados en los que el control de calidad no es homologable puede provocar situaciones catastróficas ante las que se necesita estar preparado.

Escenarios de actuación de nuestras Fuerzas Armadas y FCSE

Como consecuencia del análisis anterior, los escenarios más probables de actuación de las Fuerzas Armadas se caracterizará muy probablemente, en el medio y largo plazo por:

– Actuaciones de protección del territorio nacional, de la población y de las infraestructuras esenciales. Esto incluye la vigilancia de los

espacios de soberanía y las actuaciones en apoyo de las autoridades civiles y de los intereses nacionales
– Actuaciones en el ámbito internacional mediante la participación en operaciones en el exterior como parte de fuerzas empleadas por organizaciones internacionales.

De forma desglosada, las implicaciones de lo anterior quedan así.

1. En el ámbito nacional:
   – Defensa del territorio nacional mediante la presencia de fuerzas y la capacidad de disuasión, basada entre otros factores en la superioridad tecnológica, etc.
   – Vigilancia y control de los espacios de soberanía terrestres, navales y aéreos. Estas actividades estarán cada vez más ligadas a unos medios tecnológicos que deberán prestar servicio no sólo a las Fuerzas Armadas y a las FCSE, sino a cualquier otra autoridad del Estado que lo necesitare.
   – Defensa de los ciudadanos e intereses nacionales fuera de nuestras fronteras, en el caso de que esa defensa no pueda realizarse en el ámbito multinacional. La superioridad tecnológica en este caso permitirá compensar otros factores de planeamiento que pudieran ser adversos (situación, terreno, distancias, etc.).
   – Apoyar a las FCSE en la lucha contra el terrorismo, o en la protección de las infraestructuras esenciales en situaciones de especial riesgo, o en otras actividades que el gobierno encomiende a las Fuerzas Armadas.
   – Contribuir, junto con otras instituciones del Estado y las Administraciones Públicas, a preservar la seguridad y bienestar de los ciudadanos en los supuestos de grave riesgo, catástrofe (ya sea natural o provocada por el hombre), calamidad u otras necesidades públicas.
   – Apoyo a las autoridades civiles con diversas capacidades militares. Aparte de las capacidades empeñadas en los cometidos mencionados anteriormente, las Fuerzas Armadas pueden aportar otras capacidades en apoyo de las autoridades civiles: transporte aéreo de autoridades, participación en ceremonias, colaboración en actividades culturales y sociales, etc.
2. Con respecto a las FCSE, los escenariosmás probables, de nuevo en un horizonte de las próximas dos décadas, en los cuales deberán actuar pueden describirse de la siguiente manera:

- Las FCSE deberán responder a los problemas planteados en primera línea de costa, realizando importantes inversiones y mejoras en tecnología de vanguardia de modo constante. La prioridad se fijará en aquellas zonas de mayor incidencia.
- Se hace imprescindible que el despliegue del Sistema Integrado de Vigilancia Exterior se vaya extendiendo por todas las zonas afectadas hasta formar una gran y eficaz línea imaginaria de vigilancia y detección así como potenciar el servicio marítimo y los recursos humanos y materiales de las unidades territoriales afectadas.
- Se incrementará por parte de las FCSE la vigilancia en el perímetro fronterizo y se adoptarán requisitos más estrictos para permitir la entrada legal de personas procedentes de los principales países de origen de inmigrantes.
- La protección de infraestructuras sensibles cobrará una importancia vital. El gran impacto que una agresión a instalaciones de este tipo puede tener entre la población hace que su protección deba incluso de contar, cuando las situaciones lo requieran con el apoyo de las Fuerzas Armadas.
- Los esfuerzos de captación y análisis de información y su elaboración para prevenir el delito y diseñar metodologías y técnicas será una necesidad cada vez más importante en la que a la tecnología le cabe un papel determinante.
- Las FCSE colaborarán, como las Fuerzas Armadas, con los Servicios de Protección Civil en los casos de grave riesgo, catástrofe o calamidad pública.

3. Y en el ámbito multinacional:
   - Proyección del poder militar. Con esto se entiende la capacidad para influir en zonas en crisis mediante el despliegue de capacidades militares de acuerdo con los intereses nacionales de seguridad. En este tipo de a actuaciones, la superioridad tecnológica es un posibilitador de las operaciones.
   - Contribución a la defensa de un país aliado en el marco de la Organización del Tratado del Atlántico Norte (OTAN), en caso de necesidad. Las operaciones en el marco de la OTAN exigen unos estándares tecnológicos comparables a los de nuestros aliados.
   - Operaciones para garantizar la continuidad de los suministros de recursos básicos.

– Operaciones para evacuar nacionales, o ciudadanos de países amigos y aliados, de zonas en crisis. Relacionado con el cometido «defensa de los ciudadanos e intereses nacionales fuera de nuestras fronteras» en el ámbito nacional es de aplicación en el campo tecnológico lo mismo que en ese ámbito de actuación.
– Operaciones de apoyo a la paz. Bajo mandato de Naciones Unidas, las Fuerzas Armadas españolas podrán integrarse en fuerzas multinacionales con el objetivo de prevenir un conflicto armado, o, una vez iniciado éste, imponer la paz, o bien contribuir a su mantenimiento y consolidación tras un acuerdo entre los beligerantes. Es quizá en este campo donde la sinergia entre el usuario y las tecnologías de vanguardia que España está preparada para aportar en el medio y largo plazo sea más evidente.
– Operaciones militares para la lucha contra el terrorismo, la proliferación de armas de destrucción masiva o la delincuencia organizada. Éste es uno de los campos en los que de manera más obvia, la cooperación entre las Fuerzas Armadas y las FCSE, incluso en el exterior, se hace más necesaria, evidenciando el carácter continuo de la seguridad nacional.
– Las intervenciones militares pueden realizarse también en apoyo a las FCSE en la lucha contra redes de tráfico de armas, narcóticas o personas.
– Operaciones de ayuda humanitaria, para minimizar las consecuencias de conflictos armados o catástrofes naturales sobre la población civil. Se materializan normalmente mediante el apoyo al gobierno de los Estados afectados, o a las agencias de Naciones Unidas, con diferentes capacidades militares.
– Operaciones de observación de los acuerdos de paz o de los derechos humanos. Con el despliegue de las FCSE en los países inmersos en estos procesos.
– Operaciones de asesoramiento policial, e incluso con misiones ejecutivas. En las cuales las FCSE aporten su nivel tecnológico y contribuyan al resurgir de la nación involucrada en cualquier tipo de conflicto.
– Operaciones en las que se aporte seguridad a una zona determinada, instalaciones, personalidades, al propio gobierno, etc. ayudando a una posible transición en un entornoseguro y estable en el que se pueda desarrollar.

IMPLICACIONES EN EL DESARROLLO DE LAS CAPACIDADES PARA COMBATIR LAS FUTURAS AMENAZAS

De todo lo analizado en el capítulo anterior se deben extraer una serie de implicaciones para el desarrollo de capacidades que dotando las Fuerzas Armadas y las Fuerzas y Cuerpos de Seguridad del Estado (FCSE), y por qué no, a cualquier agencia u organismo del Estado que lo requiera dentro de ese contexto coordinado al que se viene aludiendo desde el principio.

Para solventar con éxito los compromisos que los escenarios de actuación descritos anteriormente plantean, las Fuerzas Armadas y las FCSE se deberán dotar de unas capacidades que están constituidas por la agrupación coherente de:

- Medios materiales.
- Infraestructuras.
- Recursos humanos.
- Adiestramiento.
- Doctrina de empleo.
- Organización.

Si bien es evidente que el enfoque de este capítulo se centra en el papel que la tecnología aplicada pueda tener en el éxito sostenible en escenarios y con retos muy variados, lo cierto es que el déficit en alguno de los puntos anteriores puede comprometer hacer aumentar el riesgo de fracaso hasta extremos inaceptables. A continuación se van a exponer unas características, que sin llegar por supuesto constituir requisitos operativos o técnicos de ningún equipo o tecnología, deben informarlos en todo el espectro de actuación y a lo largo del tiempo.

Medios materiales

Las tecnologías que se adopten (y adapten) para dotar a las Fuerzas Armadas y las FCSE deben cumplir unos requisitos en las facetas operativa, logística y de seguridad de su empleo.

1. Operativamente:
   - Deben proporcionar una superioridad en el combate –una de las grandes áreas de capacidad adoptadas por España y por la Organización del Tratado del Atlántico Norte (OTAN)– que incluso tienda a la «supremacía», al menos de carácter local.
   - El equivalente a la superioridad en el combate, en caso de lucha contra la delincuencia, podemos situarlo en el dominio del escenario y en control de personas, entornos y situaciones que por un lado permitan prevenir, atajar o combatir el delito así como acumular la información necesaria para permitir la acción eficaz de la Justicia.
   - Su operación y manejo debe requerir las menores adaptaciones orgánicas posibles, viniendo a integrarse también en las estructuras ya existentes.
   - Deben permitir el mayor grado de interoperabilidad con los aliados, siempre en permanente compromiso con la seguridad.
   - En el mismo sentido que se comentaba anteriormente, la interoperabilidad referida al ámbito de la seguridad ciudadana debe cristalizar en la posibilidad de afrontar con éxito las actuaciones de cooperación internacional en las que nuestras FCSE se van a ver inevitablemente implicadas en las próximas décadas.
   - La disposición de información puede crear el espejismo de que todo es controlable desde los más altos niveles de conducción. Las nuevas tecnologías que desde el campo de la seguridad transfronteriza se incorporen a las operaciones militares o de seguridad ciudadana deberán facilitar la toma de decisiones en los niveles adecuados.
   - Las redes de telecomunicaciones y los sistemas de información se constituyen no sólo en los auténticos «esqueletos» del dispositivo operativo sino en su sistema circulatorio. Por lo tanto, como a este aumento de su valor cualitativo le acompañará un aumento en el consumo de recursos operativos (ancho de banda, necesidades de encriptación, *hardware* apropiado, etc.), el planeamiento de los sistemas de telecomunicaciones e información deberá ser efectuado probablemente al más alto nivel, con el objeto de optimizar las

capacidades existentes. Este hecho no debería impedir una gestión y un empleo descentralizado y adaptado a las necesidades del comandante o agente en contacto, verdadero usuario final del dispositivo, a partir de ahora.

2. Logísticamente:
   - Las tecnologías y los equipos que se diseñen y adquieran deberán prestar mucha atención a su movilidad, facilidad para ser proyectados y simplicidad en el mantenimiento.
   - La vertiginosa capacidad de cambio y evolución de tecnologías y sistemas obliga a que en todo aquello que sea posible, los equipos estén escalables y actualizables hasta donde la eficiencia económica lo permita.
   - La formación del personal de mantenimiento debe ser rápida, basando éste en la mayor medida posible en procedimientos de sustitución por módulos.
   - La persistencia en el tiempo de los escenarios descritos anteriormente y el alcance de este análisis obliga a prever unos escenarios presupuestarios estables, que permitan un esfuerzo sostenido en la fase de obtención del recurso en el ciclo logístico.
3. Seguridad:
   - La seguridad será un requisito variable. Las acreditaciones deberán ser las necesarias. Habrá que prestar tanta atención a la seguridad como lo requiera el escalón correspondiente de empleo.
   - La seguridad en los equipos tenderá a ser de manera que ni su gestión, ni su empleo de ancho de banda o recursos de proceso comprometan la eficacia del sistema.

Infraestructuras

Los medios materiales que doten a las Fuerzas Armadas y las FCSE en el medio y largo plazo y que integren tecnologías vanguardistas en las cuales la industria y la universidad españolas aporten gran valor añadido deberán ir acompañadas por las infraestructuras de gestión logística, de formación y de adiestramiento necesarias.

De nuevo, un horizonte temporal lejano implicará un esfuerzo de planificación riguroso con criterio de flexibilidad que permitan que las inversiones en infraestructura, muchas veces las más costosas, no se vean desbor-

dadas por un cambio del entorno. Así, las líneas directrices en este campo bien pudieran ser las siguientes:

- Construcción de edificios de utilidad logística multiusos, configurables y de geometría adaptable en lo posible.
- Especial hincapié en las infraestructuras que también sean dedicadas a la simulación.
- Dotación económica para mantenimiento en un escenario estable.
- Optimización de los centros e instalaciones científicas públicas y búsqueda de sinergias con empresas, universidades y otros centros de investigación.
- Búsqueda de la economía de escala y análisis de acuerdos nacionales con otras Administraciones del Estado y en el ámbito internacional para optimizar recursos.

Recursos humanos

No cabe discusión sobre el valor clave de este componente. La persona, como base y beneficiario de todos los equipos puestos a su disposición tiene que constituir el centro del diseño, la planificación y el empleo de las tecnologías.

Sobre el personal como componente axial de una capacidad operativa hay que abordar, al menos, las siguientes facetas: la formación, el empleo, la mentalidad y la motivación:

1. *Formación*. La formación es la única manera de materializar la superioridad que reclamábamos en el campo operativo. Sin ella la tecnología no es capaz de entregar todos los beneficios. La formación del personal que manejará y operará los equipos tecnológicos en las próximas dos décadas debería transitar por las siguientes vías:
   - Reorganización y unificación de todos aquellos centros de formación tecnológica en las Fuerzas Armadas y en las FCSE de manera que la organización en una primera fase se haga en función de la materia, y no del usuario. Como la formación siempre constará de una parte tecnológica y otra operativa, será en esta última donde se produzca la diferenciación por usuario que inevitablemente debe darse. Este campo, el de la racionalización de los centros de formación tecnológicos es probablemente uno de los que más recorrido

tienen y uno de los que más sinergias pueden extraerse en ese enfoque de armonización de funciones entre las Fuerzas Armadas y las FCSE por un lado, y con la universidad por otro.

– La formación debe diseñarse de manera que a la complejidad creciente de los sistemas no le acompañe esa misma complejidad en la formación para la operación (y ya vimos que tampoco para el mantenimiento) de los equipos.
– El diseño de los planes de formación es una responsabilidad compartida entre el usuario, el diseñador y el fabricante. Una aproximación exitosa en el largo plazo debe conseguir que desde las primeras fases del diseño, el usuario esté implicado e integrado en los equipos humanos que definan los parámetros que afectarán a la formación.

2. *Empleo*. El empleo de equipos y tecnologías de vanguardia en entornos operativos exigentes obliga a adoptar una serie de premisas en la preparación de la fuerza. Los operadores deberán seguir procesos que apunten hacia:
   – Especialización. Los operadores de equipo deberán complementar su formación técnica común, impartida probablemente en centros y con planes compartidos por todos los usuarios con la formación táctica u operativa que les habilite para ser ellos los materializadores de la superioridad que se persigue.
   – Aptitud táctica y operativa. Los operadores de equipos tecnológicos trabajarán integrados en unidades y agrupaciones más amplias a cuyos cometidos ellos respaldan, desarrollando tareas de apoyo. Este personal debe ser capaz de seguir en todo el espectro operativo a las fuerzas a las cuales apoyan.
3. *Mentalidad y motivación*. El empleo de equipos y tecnologías de vanguardia es una realidad consolidada en nuestras Fuerzas Armadas y FCSE. Unas instituciones que no están al margen del progreso de las sociedad española. En los próximos 15 a 20 años este fenómeno se afianzará. El salto tecnológico que aún afecta al personal de las Fuerzas Armadas y las FCSE en tanto que «inmigrantes digitales» se irá desvaneciendo al ritmo al que cada vez más componentes de estas organizaciones sean «nativos digitales». Aún así, en el corto plazo y con ánimo de proyección hacia el futuro, es inevitable que las tecnologías se conviertan en un factor de planeamiento inevitable, que condicionen las posibilidades y por lo tanto terminen por condi-

cionar las formas de pensar. Las distintas percepciones del espacio y el tiempo, el valor de la comunicación y el tratamiento y gestión de la información modelan unas dinámicas de pensamiento distintas entre aquellos que adaptan sus ideas a la tecnología y aquellos que piensan tecnológicamente. Por lo tanto, en el plano de los recursos humanos y el campo de la mentalidad habrá que hacer un esfuerzo (que irá haciéndose innecesario con el paso del tiempo) para acompasar las velocidades y las lógicas de pensamiento con las posibilidades que proporcionan las tecnologías. El segundo aspecto a considerar, *la motivación*, tiene un peso fundamental en la correcta utilización del personal en relación con las tecnologías. Las ideas que pueden inspirar el tratamiento de este intangible pueden ir orientadas como sigue:

– La selección debe prestar atención a las personas y perfiles más afines a los entornos tecnológicos.
– La permanente innovación y actualización que estimule el interés de manera que se eviten los largos periodos de monotonía y estancamiento, que aún en sistemas de vanguardia conducen a la desmotivación.
– Lo anterior debe conjugarse con la especialización y el dimensionamiento correcto de los periodos de tiempo dedicados a los equipos y las tecnologías. La constante mutación también conduce a frustraciones que deben y pueden evitarse de manera fácil.

Adiestramiento

El adiestramiento constituye la generalización del proceso formativo por una parte, y también el vínculo con el empleo operativo de los recursos por otra.

Según la definición tradicional, el adiestramiento se atribuye a una unidad o grupo, mientras que la instrucción (o formación, más propiamente en este caso) tiene como objeto el individuo.

Teniendo siempre presente el objetivo final de que la tecnología nos comporte beneficios operativos irrebatible tanto para las Fuerzas Armadas en operaciones como para las FCSE en el desarrollo de sus tareas, y centrando el foco en las tecnologías en las que mediante la siempre perseguida sinergia, España pueda ocupar un papel de liderazgo, es necesario, a la

hora de contemplar la obtención de capacidades las necesidades de adiestramiento que éstas comportan.

El adiestramiento deberá realizarse en dos entornos:

1. Entorno sintético: a través de simulación constructiva, virtual o en vivo.
2. Entorno real: en ejercicios o centros de adiestramiento.

La fabricación de pilotos, simuladores y centros de adiestramiento, probablemente compartidos y multifunción, deberá marcar la línea en este aspecto en el futuro.

El adiestramiento debe partir de unos supuestos doctrinales que en el nivel en el que se plantea la utilización de las tecnologías procedentes de la seguridad transfronteriza se encuentran en el nivel táctico (para las Fuerzas Armadas) o de empleo operativo (para las FCSE). En estos niveles, la experiencia de socios y aliados tiene mucho valor. Los diseñadores de los programas de adiestramiento deberán tener en cuenta, con una lógica de doble vía, los siguientes puntos:

– Cooperación con unidades y fuerzas afines de otros países que utilicen estas tecnologías.
– Oferta de instalaciones, simuladores o centros de adiestramiento a otros países con el objetivo de minimizar el impacto económico y mostrar al exterior el estado del arte y las potencialidades nacionales.

Doctrina de empleo

La doctrina es la base documental que recoge la manera de emplear una fuerza en cada una de sus capacidades. Tiene la finalidad de alinear las mentalidades, unificar los procedimientos y fortalecer la cohesión entre los miembros de una organización.

Las doctrinas son tan necesarias como dinámicas. Tal y como se señalaba anteriormente, el nivel en el que se emplearán las tecnologías objeto de este *Documento* se encuentra en el campo táctico, o de contacto, sea éste específico o conjunto.

Las doctrinas son a las organizaciones lo que la mentalidad a las personas, estructuran la manera de pensar. Las doctrinas que las Fuerzas Arma-

das y las FCSE elaboren en el horizonte temporal que abarca este capítulo deberán estar más influidas por la incorporación de nuevas tecnologías que lo que lo vienen estando hasta el presente.

Esta presencia tecnológica en los modos de hacer y de pensar deberá incorporar un hecho que aunque pueda parecer evidente, no tiene fácil su implantación: la tecnología transforma el entorno, porque lo hace con el tiempo y con el espacio, y además también nos trasforma a nosotros porque lo hace con nuestras dinámicas y con nuestras percepciones.

Particularizando para las tecnologías que provenientes del campo de la seguridad transfronteriza pueden y deban ser incorporadas a las Fuerzas Armadas y las FCSE españolas, las doctrinas (y por consecuencia los procedimientos operativos) deberían, de una manera progresiva:

– Contemplar la posibilidad de conformar el campo de batalla sin presencia propia o con presencia mucho más reducida.
– Integrar la información que proporcionan los cada vez más avanzados sensores en los métodos de planeamiento y también los ciclos de decisión.
– No perder sin embargo, la idea que las tecnologías son un medio y no un fin en sí mismas. Mantener el concepto de apoyo a la misión que vienen teniendo hasta hoy.
– Conseguir integrar funciones como la seguridad y la inteligencia con la guerra electrónica de manera que el componente básico sobre el que haya que actuar es la información, cuya obtención, elaboración, difusión, empleo, almacenamiento, transporte y destrucción son los parámetros sobre los que hay que actuar en operaciones, siendo este principio aplicable tanto en el ámbito de la seguridad como en el de la defensa.
– En relación con lo anterior, la gestión de la información irá muy probablemente implicando una gestión diferente del tiempo, de manera que de la misma manera que en el punto primero se hacía mención a la conformación del espacio de forma remota o con presencia más reducida, ahora ocurrirá con el tiempo, de manera que un apropiado manejo de la información aumente las posibilidades de simultanear acciones o de sucederlas de una manera más eficiente.

Las doctrinas, como antes se avanzaba, irán también progresivamente contemplando una evolución en la definición y cometidos de los niveles

de planeamiento y conducción de las operaciones. El aumento de información en todos los niveles de mando, no debería distorsionar los cometidos y el alcance de las decisiones que se toman en cada escalón. Lo deseable sería que los documentos doctrinales asumiesen que estos medios que con toda probabilidad van a ir teniendo más y más presencia sean considerados como un apoyo a los comandantes y agentes en contacto de manera, aunque no exclusiva, sí prioritaria.

Organización

La última pero no menos importante componente del concepto «capacidad» es la organización. La organización que debe entenderse no sólo como estructura sino también como dinámica de funcionamiento. Además la experiencia demuestra que es esta última la más difícil de depurar.

¿Cómo van a afectar los entornos estratégicos descritos, los escenarios previsibles de actuación y las tecnologías que a raíz de la experiencia nacional puedan ir incorporándose a las Fuerzas Armadas y las FCSE a la organización del sistema de seguridad nacional en España?

Una hipótesis posible, y deseable, sería que el aumento de información disponible desde los más bajos niveles hacia arriba evidencie la carencia de auténticos modelos de dirección estratégica de las organizaciones.

Pero en un nivel menor de ambición, la adquisición de capacidades basadas en tecnologías procedentes del control fronterizo no debería implicar cambios revolucionarios ni en los órganos de dirección y planeamiento, ni en la fuerza, o unidades o servicios operativos, ni en los elementos de apoyo.

Las tendencias organizativas sin embargo, también tendrían que tener en cuenta dos tipos de «líneas»: unas en sentido vertical y otras en sentido horizontal:

– Las líneas funcionales, que son las que enlazan los distintos elementos que sirven a una misma necesidad en varios niveles (y que podría representarse como una línea vertical que enhebra desde la fuerza en contacto al jefe de la organización), por ejemplo, la necesidad de vigilancia del campo de batalla o la necesidad de control y vigilancia de la frontera marítima contra inmigración ilegal o delincuencia organizada.

– Aquellas otras, que pueden disponerse en sentido horizontal, y que unen las tecnologías comunes aplicables a todas las necesidades, los sistemas de transporte de la información o, por encima, los sistemas de adquisición comunes a cualquier actor presente en el campo de batalla o ámbito de actuación de las FCSE.

Pues bien, estas «líneas», que se cruzan ortogonalmente conforman un tejido matricial que va dejando obsoleto los tradicionales sistemas piramidales aptos para organizaciones y entornos más lentos, más estables y en los cuales la cantidad de información era mucho menor y el ciclo de toma de decisiones más pausado.

En resumen, los escenarios estratégicos detallados, los riesgos y las amenazas actuales y los previsibles en los próximos 15 a 20 años así como los ámbitos en los que actuarán nuestras Fuerzas Armadas y nuestras FCSE muestran cómo existe un largo y ancho campo de aplicación de tecnologías en las que, como se viene reiterando, España ocupa una posición de vanguardia destacada en el concierto de las naciones de nuestro entorno.

Parece razonable asumir que la adopción de estas tecnologías se haga de manera metodológica, de forma que a los medios materiales les acompañe la infraestructura necesaria, los recursos humanos que puedan operarlos eficazmente, que su utilización sea llevada a cabo por unidades adiestradas de acuerdo a una doctrina acertada y común y que finalmente, sean encuadrados y organizados de forma eficiente y flexible.

Así pues, establecidos los escenarios y los retos a los que las Fuerzas Armadas y las FCSE deberán hacer frente, es necesario hacer un recorrido por las tecnologías que hoy pueden apoyarlas en solventar exitosamente esos compromisos y las que pueden hacerlo de aquí en adelante.

ANÁLISIS DE LAS TECNOLOGÍAS NECESARIAS PARA EL DESARROLLO DE LAS CAPACIDADES RELACIONADAS CON LA SEGURIDAD TRANSFRONTERIZA

Sensores

Se analizan aquí cuatro tipos de sensores adecuados a la aplicación: sensores radar, sensores optrónicos, sensores tácticos enterrados y receptores de análisis del espectro radioeléctrico.

El radar ha sido desde siempre uno de los sensores más atractivos para la vigilancia de fronteras, debido a su capacidad de operación en cualquier circunstancia ambiental (presencia de niebla o lluvia, humo, diurna o nocturna) que permiten su operatividad 7/24. A esto une su capacidad de vigilar fronteras terrestres, aéreas, fluviales o marítimas donde el despliegue de sensores de tipo táctico enterrados no es posible. Y por último es un sensor que permite alcances de hasta varios centenares de kilómetros o incluso superiores, debido a lo cual se destaca como el sensor principal en este tipo de aplicaciones, al menos para la primera detección de la amenaza, véase por ejemplo la estructura y funcionamiento del Sistema SIVE.

Sin embargo, con estas propiedades comunes, existe una gran variedad de sistemas y tecnologías con características y prestaciones diferentes. Una posible segmentación de los diferentes sistemas es en función de la frecuencia de operación. Como regla general cuanto mayor sea la frecuencia mejor es la resolución (la capacidad de separar espacialmente dos blancos próximos entre sí), menor el tamaño del equipo y menor el alcance del sistema.

En el extremo más bajo tenemos los radares OTH *(Over The Horizon)*. Estos sistemas operan en frecuencias entre 3 y 30 MHz y tienen la ventaja

de que aprovechan la reflexión de la señal en la ionosfera para conseguir alcances del orden de los 2.000 kilómetros en instalaciones al nivel del suelo. Muchos de estos sistemas se desplegaron durante la guerra fría para la detección temprana de misiles, pero en la actualidad se están empleando para la vigilancia del narcotráfico, como por ejemplo el Sistema AN/TPS-71.

A priori este tipo de sistemas resultaría muy apropiado para la detección de barcos «nodriza» a larga distancia desde por ejemplo las costas de Mauritania o Senegal. Sin embargo, hoy por hoy existen serias dificultades técnicas. La primera sin duda es el coste y aparatosidad de las instalaciones. Debido a la baja frecuencia de operación estos sistemas usan antenas en *array* que pueden tener varios kilómetros de longitud, y emiten potencias del orden del megavatio, figura 1, para poder disponer de eco suficiente (lo que a su vez plantea dudas sobre los posibles efectos biológicos sobre las personas). En un entorno de depresión económica se requeriría un abaratamiento importante de los costespara hacer viable su despliegue en Europa.

El segundo gran problema es la resolución, del orden de kilómetros. Éste es un campo en el que es previsible una importante mejora en las próximas décadas. En los últimos años se ha experimentado un tremendo avance en las técnicas de procesado digital de la señal radar y en particular en las técnicas de proceso en *array*.

Parece razonable prever que las emergentes técnicas de super resolución van a permitir mejorar las prestaciones angulares de estos sistemas de forma notable.

El tercer gran inconveniente de los sistemas actuales es la dificultad para el procesado *doppler*. Este procesado es indispensable para detectar únicamente los blancos móviles y poder separarlos de las reflexiones del propio entorno natural. En los radares OTH este problema es especialmente difícil por la baja frecuencia de operación (bajas frecuencias *doppler*) y por el efecto de dispersión doppler que produce la ionosfera. En la actualidad ya se está trabajando en solucionar este problema con la utilización de formas de onda adaptativas y es previsible que en pocos años el problema esté superado.

En el otro extremo del espectro radioeléctrico están los radares de milimétricas. En este caso se trata de sensores que pueden hacerse muy compactos y disponen de una muy elevada resolución, lo que permite obtener pseudoimágenes de los blancos.

Su limitación fundamental es el alcance que sólo puede ser pequeño o moderado (decenas de kilómetros). Debido a ello una combinación muy in-

Figura 1.– *Sistema de antenas del Sistema relocalizable AN/TPS-71 (US Navy).*

teresante es un radar de milimétricas con una plataforma de tipo de Vehículos Aéreos no Tripulados (UAV). Una limitación actual de estos sistemas es

el elevado coste de los dispositivos, pero la tendencia es a un abaratamiento rápido debido al interés industrial de, por ejemplo, los radares anticolisión para coches. Esto permite vislumbrar en un futuro redes de radares de este tipo vigilando de forma desatendida un perímetro fronterizo.

Los radares de milimétricas poseen una gran capacidad de análisis *doppler* de forma que son capaces de detectar móviles a muy baja velocidad (por ejemplo una persona caminando). Además le dan al operador una pseudoimagen que permite identificación del blanco, figura 2. En la actualidad se está trabajando internacionalmente en el desarrollo de algoritmos de reconocimiento automático, pero todavía los resultados obtenidos son muy pobres.

Los radares de milimétricas son por naturaleza HRR *(High Resolution Radars)*, aunque también pueden desarrollarse Sistemas HRR en bandas más bajas con resoluciones algo peores. Los radares HRR exhiben otra

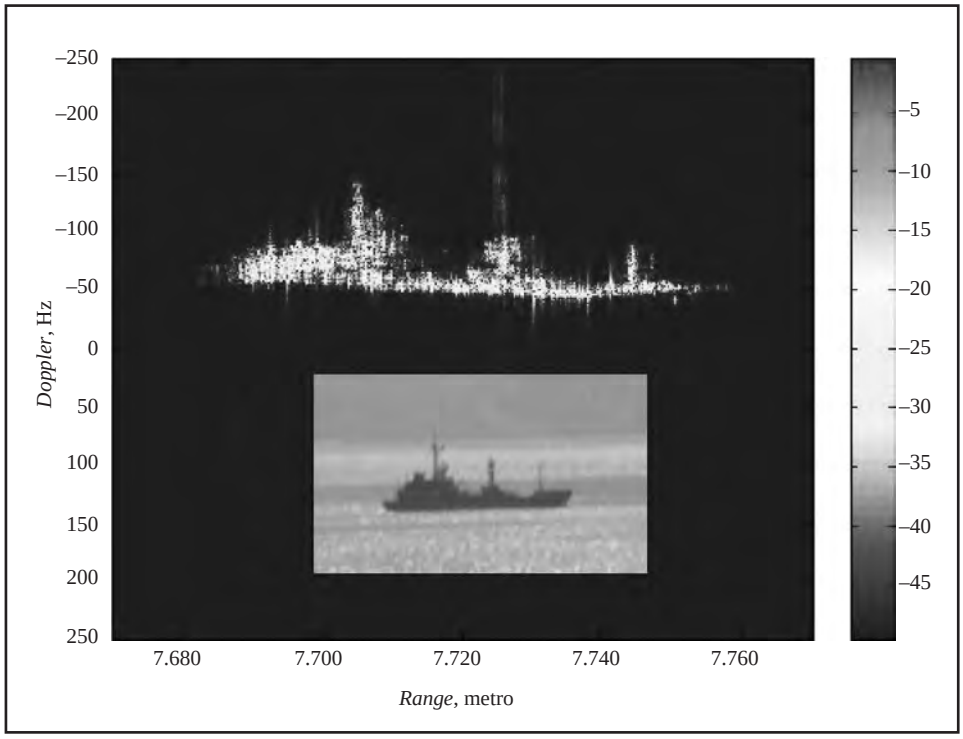

Figura 2.– *Foto de un buque e imagen obtenida con un radar de milimétricas en el estrecho de Gibraltar (Universidad Politécnica de Madrid).*

interesante propiedad de cara a la vigilancia de fronteras: la posibilidad de detección de blancos a baja cota. Es conocido que un vehículo aéreo de pequeño tamaño volando bajo es capaz de burlar la vigilancia de un radar, especialmente sobre la superficie de un mar en calma. Esto es debido, principalmente al efecto de la reflexión del eco sobre la superficie, que produce un doble camino para la señal de eco, originando una interferencia destructiva que cancela la señal en el receptor del radar. Esto puede evitarse (teóricamente) en un radar HRR ya que es capaz de separar los dos ecos (rayo directo y *multipath*) discriminándolos temporalmente. Los sistemas actuales todavía no lo consiguen en la práctica, debido a que se necesitan resoluciones mejores que las actualmente disponibles, pero es previsible que esto cambiará en unos 10 o 15 años.

También en el caso de los radares de milimétricas, las técnicas de procesado en *array* deben experimentar un gran desarrollo en los próximos años, ya que generan un pincel de antena muy fino y la capacidad de poder dirigirlo de forma ágil e inteligente multiplican las capacidades de estos sensores.

En las bandas de trabajo intermedias se pueden construir soluciones de compromiso entre las situaciones extremas analizadas. Pero lo que resulta claro es que en los próximos años será necesario un avance importante en las técnicas de alta resolución así como en las técnicas de procesado en *array*. La generación de alta potencia a costes moderados parece también otro área de importancia estratégica. En este sentido la línea de trabajo más importante es la utilización de dispositivos de nitruro de galio, que promete ser una revolución a corto plazo en la generación de potencia en bandas de microondas.

La segunda tecnología de sensores para conseguir las capacidades perseguidas son los sensores optrónicos, en particular en la banda de infrarrojos. La señal infrarroja no tiene la misma capacidad de penetración que la señal radar en la niebla o humo, pero tiene una resolución muy superior produciendo imágenes de fácil interpretación para el operador. El infrarrojo cercano tiene mejor resolución y peor capacidad de penetración, mientras que en el lejano ocurre lo contrario.

La tecnología de vigilancia infrarroja desatendida no está tan madura como la vigilancia radar, pero es un campo emergente que va a experimentar un gran avance en los próximos años. Se está actualmente trabajando de forma muy activa en algoritmos de detección y de reconocimiento automático de patrones que prometen mejorar enormemente sus prestaciones.

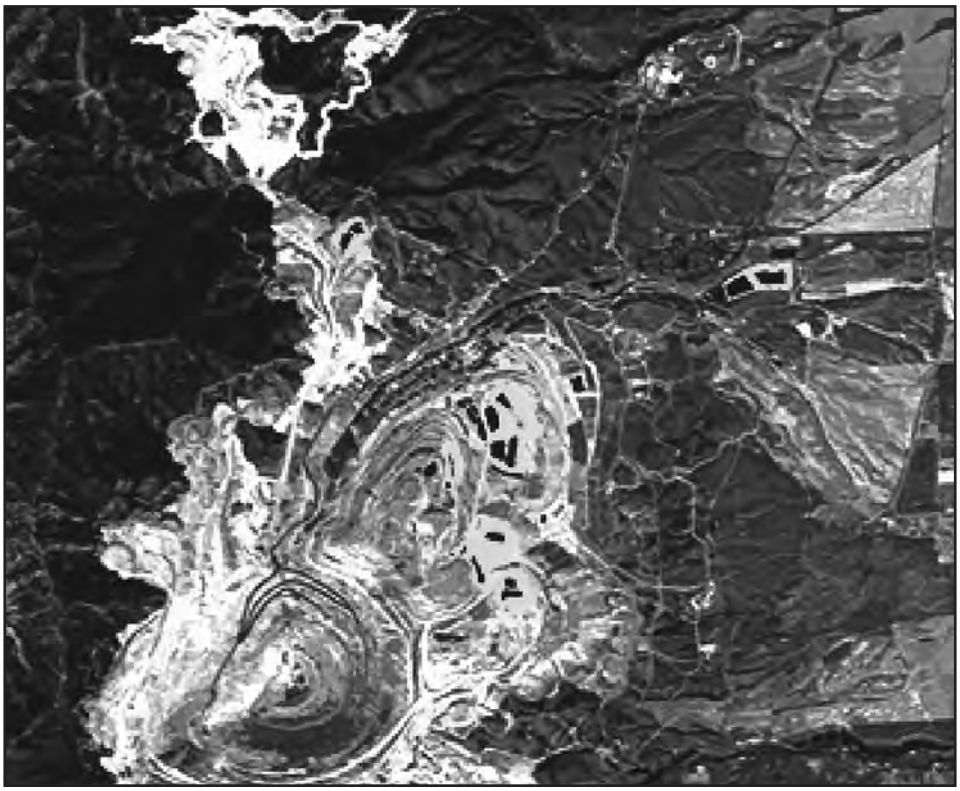

Figura 3.– *Imagen hiperespectral infrarroja de una mina en Arizona, obtenida desde una plataforma aérea (Goodrich corp.).*

Uno de los campos de más actualidad en este ámbito es el de los sensores de doble banda o multibanda, que permiten extraer más información de la escena estudiada, lo que conllevará unas distancias de reconocimiento y actuación mayores, figura 3.

En este sentido trabajan los sensores hiperespectrales que dividen la banda en trocitos de 0,01 micrometro de ancho y producen una imagen de falso color que ha demostrado mejorar enormemente la interpretación de ésta. De hecho se usan en plataformas sobre satélite ya que debido a la gran distancia, la limitación en la resolución por difracción no permite reconocer los objetos de interés si no se realiza este análisis espectral. El mayor problema de estas cámaras es su volumen y complejidad (unos 300 kilogramos en la actualidad), lo que no las hace apropiadas para aplicaciones tácticas. Éste es sin duda un campo donde se requerirá un avance

significativo en las próximas décadas. Un objetivo a medio plazo sería disponer de sensores tácticos hiper o muliespectrales con las características de portabilidad de los actuales microbolómetros.

Otra línea tecnológica de gran actividad en las imágenes de infrarrojos es el procesado digital de señal. Los avances en las Unidades Periférica del Ordenador (CPU,s) están ya permitiendo realizar en tiempo real técnicas como la ecualización de histograma o el realce de bordes que mejoran substancialmente la interpretabilidad de las imágenes por operadores humanos. El esfuerzo se enfocará en los próximos años hacia la identificación automática, si bien los progresos en este sentido son todavía lentos. Se ha avanzado algo más en algoritmos de seguimiento óptico, que ya en la actualidad comienzan a funcionar de manera fiable y que representan un paso hacia la identificación automática.

Además de las técnicas clásicas comentadas anteriormente, en los últimos años están emergiendo nuevos tipos de sensores que podrían mejorar significativamente los resultados en un futuro a medio plazo. Uno de ellos son los sensores por polarización. Se sabe que los objetos naturales emiten con una polarización homogénea mientras que los fabricados por el hombre emiten luz polarizada. Este hecho ha demostrado una gran eficacia en resultados experimentales para identificar blancos artificiales.

Otro sensor interesante es el LGICCD *(Laser Gated Intensified CCD)* que utiliza un pulso corto de iluminación y abre la cámara CCD sólo en la ventana de tiempo adecuada a un alcance predeterminado. Si el pulso es suficientemente corto podrá realizarse sinpeligro para el ojo humano, incrementando el alcance del sensor. Finalmente cabe mencionar el Ladar como posible sensor de futuro en este campo.

Sensores tácticos enterrados

Los sensores tácticos enterrados son dispositivos que incorporan sensores sísmicos y magnéticos con el objetivo de detectar las ondas de baja frecuencia que son producidas por personas andando o vehículos rodando y que se transmiten por el suelo. También detectan masas metálicas próximas tales como vehículos en paso cercano por el terreno. Habitualmente estos sensores se entierran parcial o totalmente en el terreno, son autónomos en cuanto a alimentación y disponen de un transmisor inalámbrico que usan para enviar la información de detección a un receptor lejano. Permiten

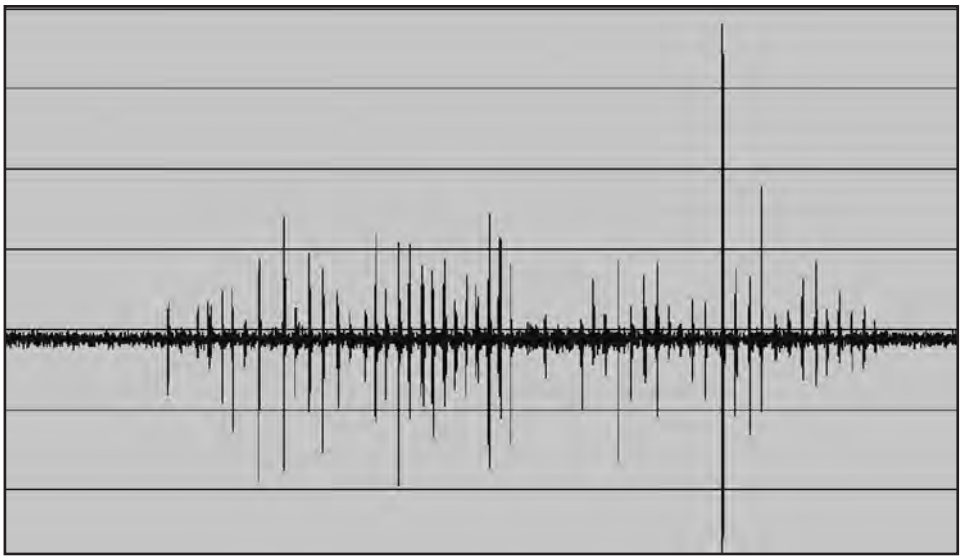

Figura 4.– *Señal producida por una persona a siete metros.*

completar otros sistemas de detección como radares o vídeovigilancia en zonas donde los anteriores sistemas son inviables o costosos, por ejemplo en zonas donde no haya cobertura de radar, figura 4.

Estos sensores han sido utilizados tradicionalmente por las Fuerzas Armadas para la detección de movimientos de tropas y vehículos en el campo de batalla y eran desplegados y enterrados durante un periodo de pocos días durante operaciones concretas. Hay también soluciones que eran lanzados desde el aire con pequeños paracaídas y se hincaban en tierra y comenzaban a operar inmediatamente.

El problema de estos sensores era la corta duración de su batería y la alta probabilidad de falsa alarma debida a su escasa capacidad de discriminación entre personas y animales o sucesos naturales, como la caída de piedras o ramas en el terreno e incluso las ondas sísmicas producidas por las raíces de los árboles en días con mucho viento.

En la actualidad se están acometiendo desarrollos de nuevos sensores tácticos enterrados, que utilizan acelerómetros de estado sólido de alta sensibilidad y arquitecturas de despliegue en red para reducir las falsas alarmas y resolver el problema de discriminación.

La arquitectura típica de las nuevas soluciones de sensores tácticos enterrados es la de una red inalámbrica de nodos sensores, un nodo router y

un centro de control remoto. Los nodos sensores inalámbricos son desplegados bajo tierra formando una barrera perimetral, encargados de detectar las intrusiones producidas dentro del área protegida. Para realizar esta función los nodos disponen de dos tipos de sensores, un sensor sísmico que identifica las ondas sísmicas producidas por el paso de una persona o vehículo, y un sensor magnético que mide las variaciones del campo magnético producidas por una masa de metal en movimiento tales como un vehículo.

El nodo router es al que se conectan los nodos sensores y se encargan de enrutar las alarmas de detección enviadas por éstos al centro de control. Los nodos routers irán desplegados a una determinada altura (asintóticamente igual a tres metros) para una correcta comunicación con los nodos enterrados. Y finalmente, en el centro de control se concentran todas las alarmas producidas con el objetivo de eliminar falsas alarmas, clasificar amenazas (vehículos o personas), y realizar su seguimiento. La figura 5 muestra la arquitectura de la red de sensores.

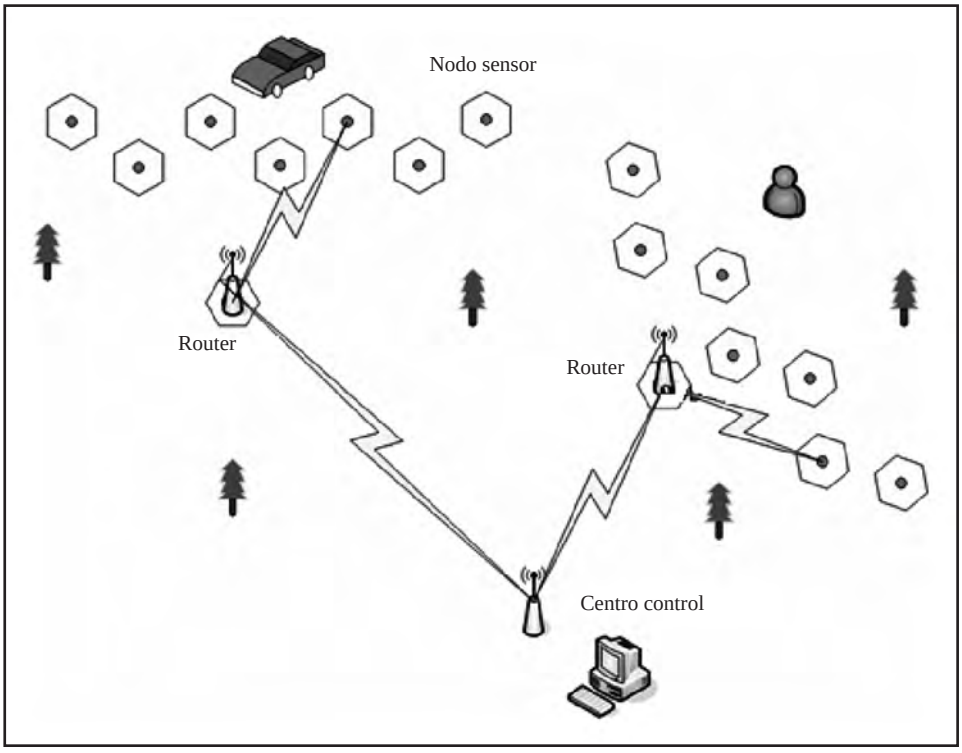

Figura 5.– *Arquitectura de la red de sensores.*

Separar y clasificar la señal producida por personas y vehículos del ruido producido por otros elementos ambientales es una tarea difícil que requiere el desarrollo de un algoritmo robusto que maximice la distancia de detección y reduzca la tasa de falsa alarma. Una posibilidad es que los propios nodos implementen un algoritmo de detección CFAR *(Constant False Alarm Rate)* que les permita autoajustarse a las distintas condiciones ambientales (lluvia, viento, etc.). Para ello los nodos ajustan, de forma automática el umbral de detección en función de la varianza de la señal obtenida, esto permite en todo momento al nodo conocer el nivel de ruido existente. Una vez producida la superación del umbral, la decisión de generar una alarma de detección es tomada utilizando el criterio de Neyman-Pearson, el cual optimiza la probabilidad de detección fijada una determinada probabilidad de falsa alarma:

– Características a 7 metros: PD >95%; PFA $<10^{-3}$.
– Características a 10 metros: PD >85%; PFA $<5 \cdot 10^{-3}$.

Otro aspecto muy importante es la reducción del consumo de los nodos sensores para poder utilizar baterías como fuente de alimentación y conseguir una autonomía de varios años. Para conseguir autonomías mayores de dos años, aparte de utilizar componentes de bajo consumo, se han aplicado varias técnicas:

– Transmisión no periódica. Sólo se envían mensajes de alarmas de detección cuando éstas se producen, además de un mensaje de información de estado del nodo cada 15 minutos.
– Recepción periódica. Los nodos son configurados para activar su recepción unos pocos milisegundos cada cierto periodo de tiempo. Por ejemplo se pueden configurar estableciendo tiempos de escucha de 5 milisegundos cada 250 milisegundos, consiguiendo así un ciclo de trabajo de un 2%. Lógicamente el transmisor deberá retransmitir el mensaje hasta que el receptor notifique su entrega correcta.
– Sincronizar la transmisión de los nodos sensores con la recepción del nodo router más próximo. De esta forma evitaremos la retransmisión del mensaje por parte del nodo sensor. Para conseguir esta sincronización, el nodo router enviará un mensaje baliza cada cierto tiempo indicando el tiempo de escucha de éste.

Estas soluciones de sensores tácticos han de irse optimizando en el futuro en paralelo con el desarrollo de acelerómetros más sensible y de menor

coste y la optimización de algoritmos combinados de detección y de reducción del consumo. Así, estas redes de sensores se postulan como la mejor solución de sensores de alerta temprana en fronteras no reguladas terrestres, de orografías montañosas y boscosas muy complicadas para radares o cámaras de vigilancia.

Sensores de vigilancia espectral

Por último mencionar otra tecnología de sensores que si bien no está encaminada a la detección directa de personas o vehículos transitando un área, sí puede servir de apoyo en la vigilancia de fronteras: la vigilancia espectral. La última década ha significado un avance espectacular en la tecnología de vigilancia espectral basada en recepción digital. La aparición a principios de la década de conversores A/D con más de 1 GHz de frecuencia de muestreo y suficiente margen dinámico han resultado ser una tecnología habilitadora para realizar vigilancia del espectro de comunicaciones que en ese mismo periodo ha pasado de abarcar sólo 2 GHz a los 6 GHz que se prevén en un futuro casi inmediato. Afortunadamente la tecnología de digitalización está avanzando a un ritmo similar y se prevé la existencia de conversores adecuados, con más de 10 GHz de muestreo para la próxima década.

El objetivo de la vigilancia espectral es en primer lugar la detección de la existencia de comunicaciones, en segundo lugar su clasificación para determinar si son potencialmente hostiles. Un paso más de explotación de la información sería descodificarlas para obtener la señal de voz o texto (por ejemplo mensajes SMS) y en último término el reconocimiento de palabras que puedan encubrir intentos de violación fronteriza. En el mundo de hace una década todas esas tareas podían ser realizadas por un equipo de lingüistas que disponían de escáneres espectrales, que demodulaban una señal analógica y la interpretaban. En el actual mundo de las comunicaciones digitales, con cifrado y alta densidad de emisiones, será necesario automatizar lo más posible esos procesos.

Cada uno de ellos significa un estadio de procesado digital diferente, y progresivamente más complejo. Aquí es donde se encuentra el cuello de botella de la tecnología actual, que no es capaz de procesar toda la información generada por los digitalizadores más veloces. Incluso teniendo en cuenta que en estos años se ha vivido una explosión de las tecnologías

FPGA *(Field Programmable Gate Array)*. Será necesaria otra explosión tecnológica similar en los DSP *(Digital Signal Processors)* o CPU,s de propósito general si se desea automatizar todo el proceso y mantener una vigilancia del 100% de tiempo real.

La detección y clasificación de señales de comunicaciones son dos procesos actualmente inseparables. Esta cadena de conocimiento de las señales presentes en el ambiente debe continuar con la identificación de dichas señales y, si es posible, de la plataforma que las ha emitido (geolocalización pasiva). Las técnicas TDOA y FDOA se utilizan actualmente de forma conjunta para la geolocalización pero en el futuro será muy probablemente el proceso en *array* la tecnología dominante.

Bibliografía

ABOELAZE, M. and ALOUL, F.: *Current and Future Trends in Sensor Networks: a Survey,* Internacional Conference on Wireless and Optical Communications Networks, 2005.

CAMPO, A. B. del; LÓPEZ, A. A.; NARANJO, B. P. D.; MENOYO, J. G.; MORAN, D. R. and DUARTE, C. C.: «CWLFM millimeter-wave radar for ISAR imaging with range coverage», *Proceedings IEEE International Radar Conference*, pp. 933-938, 9-12, mayo de 2005.

FABRIZIO, G. A.: «Over the horizon radar», *Radar Conference*, Radar'08, IEEE, pp. 1-2, 26-30, mayo de 2008.

FERMIONICS CORPORATION: página *web: www.fermionics.com*

Introduction to Sensors Systems, S. A., Hovanessian. Artech House.

JELALIAN, Albert V.: *Laser Radar Systems,* Artech House.

KIM, S.; PERGANDE, A. and HUGHEN, J.: «Low cost ka band SAR/ISAR for UAV applications», *Proceedings of the 2003* IEEE Aerospace Conference.

SENSORS UNLIMITED: página *web: www.sensorsinc.com*

SOFRADIR: página *web: www.sofradir.com*

Vectores

Es indudable que en buena parte, el éxito de los sensores anteriormente descritos depende de las plataformas usadas para desplegarlos. Se analizan aquí tres tipos de plataformas apropiadas para embarcar sensores de vigilancia de fronteras: satélites, UAV,s y globos aerostáticos.

Las plataformas satelitales ofrecen como ventaja la capacidad de operación 7/24, la capacidad de transportar varios sensores (típicamente radar, electroópticos y sensores de vigilancia del espectro electromagnético) y la capacidad de vigilar grandes áreas de terreno (cientos de kilómetros). Las desventajas principales son el coste del lanzamiento (unos 7.000 dólares/kilogramo) y la discontinuidad en el tiempo sobre una zona dada.

Aunque en los Tratados SALT I se planteaba el acceso abierto a la información sobre los programas de desarrollo de satélites de vigilancia, la realidad es que los programas siguen siendo clasificados y no es fácil conocer las capacidades tecnológicas reales de las grandes potencias. Hay siete tecnologías que resultan clave para cualquier avance en este campo: las tecnologías de propulsión, la de alimentación, la de comunicaciones, la de navegación y posicionamiento, la de encriptado, la de procesado y las de sensores. En todas ellas se han realizado avances significativos en los últimos años.

En función de la altura de la órbita los satélites se clasifican en:

- Geoestacionarios: posicionados sobre el ecuador a 35.768 kilómetros de altura. Permanecen estáticos sobre una zona concreta de la Tierra. Con tres satélites de este tipo se puede cubrir toda la Tierra excepto los polos. La desventaja principal es la distancia y el tipo de sensores que pueden usarse. El límite por difracción de los sensores ópticos es de una resolución de 10 metros y no es posible realizar radares de imagen.
- MEO: órbita media (9.600 a 19.300 kilómetros). Los límites por difracción óptica así como por atenuación en los sistemas radar siguen siendo excesivos para aplicaciones de vigilancia.
- LEO: órbita baja (160 a 1.000 kilómetros). Son los más adecuados. Es la tecnología utilizada en los satélites espía ampliamente empleados durante la guerra fría. Son capaces de dar la vuelta a la Tierra en aproximadamente una hora y media, mediante órbitas Norte-Sur que pasan por los polos. En lo que sigue nos centraremos en este tipo de plataforma.

Este tipo de satélites representa una ventaja en términos de sensores debido a la menor distancia. Permiten muy alta resolución en sistemas ópticos con aperturas de lente viables. El límite por difracción en visible para una lente de 2,5 metros de diámetro, por ejemplo, es de 7 centímetros a 250 kilómetros de altura. Eso permite obtener imágenes ópticas con muy buen

detalle. Igualmente, los sensores radar y radiométricos se benefician de una atenuación relativamente baja. Si bien el tiempo de iluminación de la franja es pequeño lo que limita la resolución máxima en los sensores SAR.

Los satélites de vigilancia LEO suelen describir una órbita síncrona con el Sol (heliosíncrona), de tal forma que el satélite pasa sobre la zona de interés aproximadamente a la misma hora local cada día. Para optimizar la iluminación y minimizar los efectos de sombras, esta hora suele ser sobre las diez antes del meridiano o las dos después del meridiano. Es decir, que un satélite genera vigilancia de una zona concreta durante unos minutos cada 24 horas. Este hecho puede ser conocido por las mafias que se dedican al tráfico de personas, evitando esas horas concretas para violar pasos fronterizos. Por otra parte, la mitad de cada órbita polar heliosíncrona se pierde para el sensor óptico visible, al estar en zona nocturna. La razón de sincronizarse con el Sol está asociada a la utilización de sensores ópticos pasivos. Esta limitación no existe si el satélite va equipado con sensores radar, que no requieren de una fuente de luz externa. Un objetivo tecnológico claro es el desarrollo de sensores SAR de alta resolución que puedan proporcionar imágenes de resolución comparable a la óptica, posiblemente mediante el empleo de frecuencias más altas y procesado de superresolución.

Hay también que tener en cuenta que un cuello de botella importante en los satélites es la disponibilidad de potencia, que limita mucho las capacidades de los sensores radar, que son bastante demandantes en este sentido, tanto para el transmisor como para el procesador. En este sentido se hace necesario el desarrollo de paneles solares más eficientes. El estado del arte actual es una eficiencia AMO *(Air Mass Zero)* del orden del 40%, utilizando tecnologías emergentes basadas en concentradores multiunión. Si se mantiene el ritmo de crecimiento actual de la eficiencia de estos paneles se esperaría llegar a eficiencias del 50% para el año 2020 y del 60% para el 2030, figura 6.

Este extremo es vital para poder integrar sensores radar con las prestaciones que requiere la aplicación de vigilancia fronteriza. En la actualidad algunos satélites utilizan *thrusters* basados en XIPS *(Xenon Ion Propulsion System)*. Es un combustible en forma de gas que pesa mucho menos que el combustible líquido habitual y es 10 veces más eficiente. Sin embargo, esto claramente limita la vida útil del satélite, o al menos la necesidad de un mantenimiento periódico. Debe tenerse en cuenta que la altura de los satélites LEO coincide con el margen de alturas que el Transbordador Espacial (STS) estadounidense es capaz de alcanzar (hasta 1.000 kilómetros).

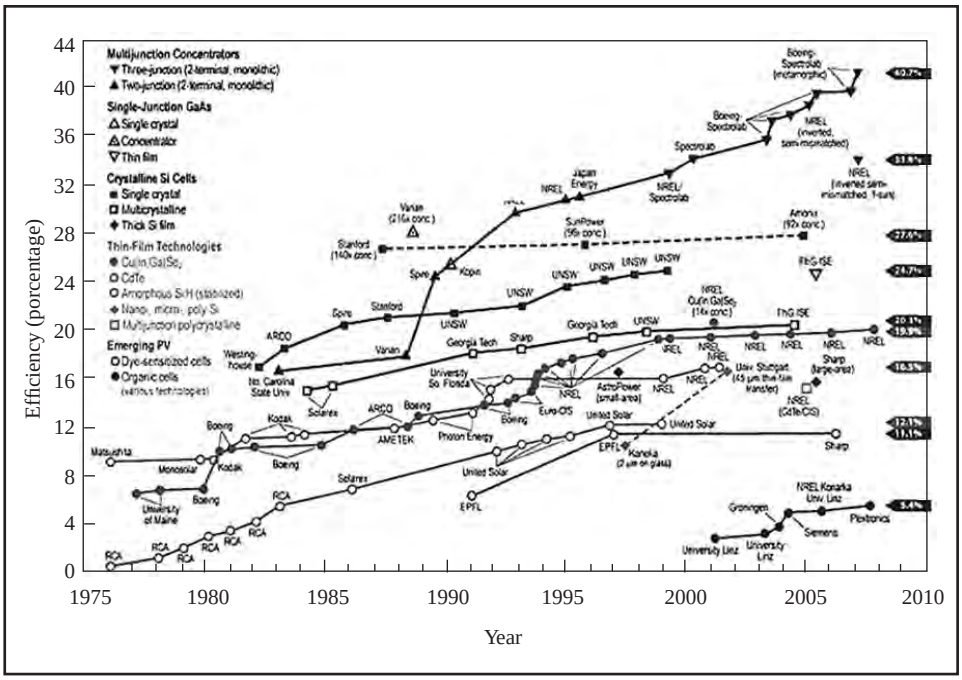

Figura 6.– *Evolución de las eficiencias de las células fotovoltaicas para satélites.*

Por último decir que existen y han existido satélites de observación civiles comerciales, cuya información puede ser comprada y utilizada por grupos terroristas o países enemigos que carezcan de satélites espía propios. Estos sistemas pueden plantear un peligro, ya que aunque el enemigo no dispondrá de la información en tiempo real, pueden ser aún útiles para planear una agresión. Sistemas como LandSAT en el año 1970 con 50 metros de resolución o SPOT en el año 1980 con 5-10 metros de resolución. En el año 1990 Israel e India lanzaron sistemas con 5 metros de resolución, y a mediados de los años noventa Rusia comercializó satélites espía con dos metros de resolución. En el año 2007 Alemania ha lanzado el *TerraSAR-X* con menos de un metro de resolución.

En cuanto a las plataformas de tipo UAV, señalar en primer lugar que es una tecnología bastante reciente y como tal es donde previsiblemente se van a lograr los avances más importantes en las próximas décadas. Los UAV,s permiten superar las limitaciones de disponibilidad de los satélites (hay que esperar a que la órbita sobrevuele la zona de interés) ya que pueden ser dirigidos a la zona de conflicto a voluntad. También limita el coste,

ya que existen UAV,s de tamaño pequeño cuyo coste es perfectamente asumible por países como España (véase el desarrollo del Programa SIVA o el más reciente proyecto Atlante).

Los UAV,s también presentan ventajas frente a las plataformas aéreas convencionales tripuladas. Entre ellas pueden citarse:

- Duración de vuelo mayor (no depende del factor humano).
- Reducción de costes (piloto, mantenimiento, etc.).
- Capacidad de operación en condiciones adversas sin riesgo de vidas humanas.
- LPD: motor eléctrico poco ruidoso, pequeño tamaño (RCS baja), con capacidad de operación subsatelital (alturas muy elevadas).

El control de vuelo más básico es el modo preprogramado. Es el método más simple, no presenta muchas dificultades técnicas, ni depende de enlaces de comunicaciones entre la estación base y el UAV, que pueden estar sujetos a ruido y/o interferencia. Con este método se puede operar a grandes distancias, fuera de la línea de visión directa entre estación base y radar. Sin embargo, el sistema es inflexible, una vez que el UAV comienza su vuelo, siguiendo ciertos puntos de control, no puede modificarse, de tal forma que no es posible realizar segundas pasadas sobre zonas interesantes. Además, si el UAV necesita volar bajo, se debe tener información precisa de la orografía del terreno. En el caso de hostilidades este método de operación no tiene capacidad de reacción ante ataques enemigos.

El modo basado en control remoto es el más común. Por medio de un enlace radio, el operador recibe datos de vuelo del UAV y envía comandos de vuelta para controlar la aeronave. La principal desventaja de este sistema es el enlace de comunicaciones radio, ya que el alcance de este enlace es el factor que limita la distancia de operación del UAV. Los sistemas más avanzados utilizan enlaces radio indirectos (vía satélite, o redes de UAV,s).

Los sistemas completamente autónomos no son, todavía, una opción viable con la tecnología actual, si bien es un campo de gran actividad en el sector. Este tipo de sistemas llevarían a bordo equipos y sensores que permitieran al UAV tomar decisiones por sí mismo, reaccionando ante ataques, o haciendo varias pasadas en una posible zona de interés. Debe también decirse que un objetivo a corto plazo es el establecimiento de una normativa que permita el vuelo de estas plataformas en el espacio aéreo no segregado, ya que existen sistemas a nivel de prototipos, desarrollados por empresas o organismos de investigación y desarrollo que están a la espera de conocer

los sensores que se requerirán para poder lanzar los programas de desarrollo. Por ejemplo, parece caro que se va a exigir un sistema de *Sense & Avoid* pero todavía no se conocen las especificaciones del mismo.

Actualmente, la diversidad de UAV,s oscila desde vehículos extremadamente simples, de bajo coste, pequeño tamaño y corto alcance, utilizados para aplicaciones de corta duración, a aviones de varios millones de euros, con inteligencia artificial, capacidad para llegar a cualquier parte del Globo, volando durante largas jornadas, y llevando a bordo una cantidad de carga útil considerable. Los UAVs más simples pueden cargar algún sensor de poco peso, típicamente, sensores térmicos o infrarrojos, videocámaras. Suelen tener un enlace de comunicaciones con una estación base a corta distancia del lugar de operación. Los más grandes suelen llevar todo tipo de sensores, entre los que se añaden radares de vigilancia superficial, y Sistemas Electrónicos de Inteligencia. Pueden comunicarse con varias estaciones base, o incluso con otros UAV,s, formando una red de comunicaciones, que permite la operación a largas distancias. El cuadro de la figura 7, p. 65, resume la segmentación de este tipo de plataformas.

La carga útil que puede transportar un UAV se ve mermada por el combustible necesario en las aplicaciones de larga duración. Siempre, se debe llegar a un compromiso entre duración del vuelo, y carga útil que puede transportarse. Normalmente, los UAV,s utilizan paquetes de misión, que incluyen los sensores y los equipos necesarios para establecer el enlace radio de datos entre los sensores y la estación base.

Muchos de los UAV,s más pequeños (mini y micro UAV) usan motores eléctricos. Este tipo de motores son mucho más silenciosos que los motores mecánicos, y por lo tanto son muy atractivos en situaciones donde sea importante no ser detectado, o en aplicaciones civiles donde no se quiera producir contaminación acústica, por ejemplo al sobrevolar parques naturales. El problema que tiene este tipo de propulsión es que debe alimentarse con baterías, placas solares y/o *fuel cells.* Este tipo de alimentación tiene menor eficiencia, y menor relación de potencia-peso, que la conseguida con motores térmicos.

Además, tiene el inconveniente de que la energía eléctrica necesaria para alimentar los sensores y sus equipos electrónicos asociados, no puede obtenerse del motor. Es por ello que el volar con motores eléctricos requiere un bajo consumo, y peso, tanto del UAV como de los sensores y equipos a bordo.

Por último, los UAV,s que llevan un mayor número de sensores, necesitan una capacidad mayor en el enlace de datos radio. Las capacidades

actuales son de 274 megabytes por segundo en el enlace de bajada, y de 200 kilobytes por segundo en el de subida. Esta capacidad es muy limitada para los sensores radar de alta resolución que potencialmente pueden llevar por lo que el desarrollo de enlaces robustos de alta capacidad es otro área interesante de investigación y desarrollo a corto plazo.

El último tipo de plataforma analizado son los globos aerostáticos y dirigibles. Un globo es en realidad un tipo especial de UAV con unas características especiales, pero que comparte con los UAV,s muchas de sus ventajas. Entre las ventajas de los globos cabe citar:

- Transporte económico (mejor tasa tonelaje/autonomía después del transporte marítimo).
- Puede transportar grandes cargas.
- Los eventuales fallos de los motores son menos críticos que en un avión.
- Pueden aterrizar prácticamente en cualquier sitio, sin requerir infraestructura importante. Tan solamente una estructura donde ser amarrado.
- Mayor autonomía, vuelo silencioso y menor contaminación.
- Capacidad de utilizar sensores SAR en dirigibles. Gran estabilidad, pocas vibraciones debido a que el régimen de trabajo de los motores y hélices es bajo.
- Resolución de los sensores fotoeléctricos mayor (también límite por difracción).
- Aumenta la línea de visión limitada por la curvatura de la Tierra

Quizá esta última ventaja sea la aplicación más inmediata y evidente. Si por ejemplo se dispone de una plataforma naval o terrestre que tiene asignada una zona de vigilancia, resulta evidente que embarcar un sensor radar o optoelectrónico en un globo anclado en el suelo y elevarlo permite pasar de tener una visión sobre el horizonte de 50 kilómetros a más de 200 kilómetros, desde una plataforma única, figura 8, p. 66.

También es necesario advertir de los inconvenientes que tiene esta tecnología. Los más destacables son:

1. Riesgo de sobrecarga por nieve o escarcha:
   - Relación volumen total/volumen de carga útil muy desfavorable.
   - Baja capacidad de maniobra.
   - Mayor vulnerabilidad a los vientos y a las condiciones meteorológicas desfavorables.

UAS: Clasificación propuesta en el JCGUAV					
Clase (MTOW)	**Categoría**	**Empleo**	**Actitud operacional**	**Radio de misión**	**Ejemplo de plataforma**
Clase III > 850 kilogramos	HALE *(High Attitude Long Endurance)*	Estratégico	Hasta 65.000 pies	Sin límite (BLOS)	 *Global Hawk*
	MALE *(Medium Attitude Long Endurance)*	Operacional/ de teatro	Hasta 40.000 pies	Sin límite (BLOS)	 *Predator B*
Clase II 160/850 kilogramos	TÁCTICO	Formación táctica	Hasta 3.000 pies	200 kilómetros (LOS)	 *Sperwer*
Clase I > 160 kilogramos	SMALL	Unidad táctica	Hasta 1.200 pies	50 kilómetros (LOS)	 *Scan Eagle*
	MINI	Subunidad táctica	Hasta 1.000 pies	25 kilómetros (LOS)	 *Skylark*
	MICRO	Táctico, pelotón, sección y personal	Hasta 200 pies	5 kilómetros (LOS)	 *Black Widow*

Fuente: Dirección General de Armamento y Material.

Figura 7.– *Clasificación de los UAV¸s.*

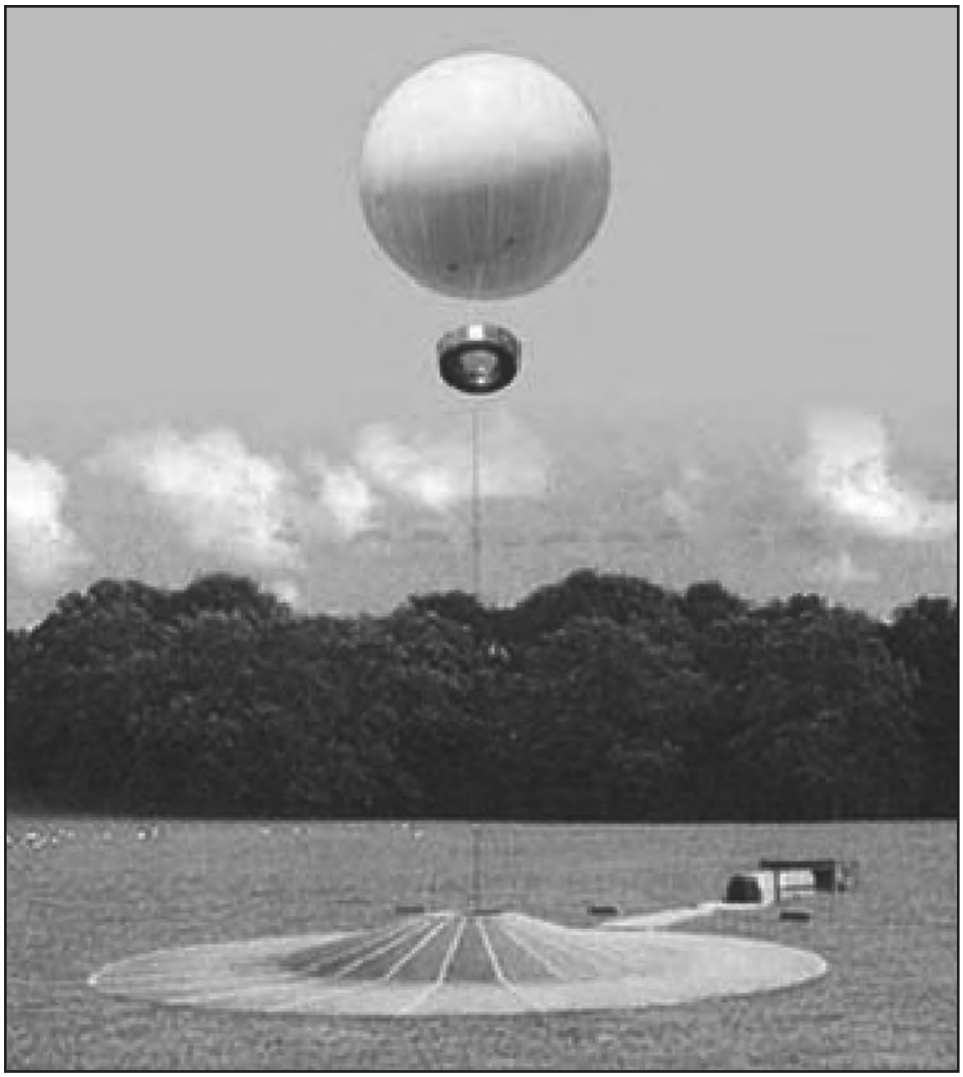

Figura 8.–*Globo aerostático anclado, con sensores.*

– Poca altitud de vuelo. Aunque se están investigando globos capaces de ponerse en órbita.
– Velocidad de vuelo baja.

2. Las características típicas de una plataforma dirigible actual son:
   – Velocidades:10-130 kilómetros/hora.

– Altitud: 15-3.000 metros.
– Autonomía: 15-20 horas. Existen modelos que pueden repostar en vuelo y permanecer volando un mes de forma continuada.
– Costes de operación y mantenimiento de un dirigible: 110-170 dólares/hora vuelo.
– Capacidad de carga: desde varios kilogramos a alguna tonelada.

En todos estos campos son previsibles mejoras en los próximos años. Los aeróstatos modernos, amarrados a tierra, pueden permanecer meses en el aire, hasta que reciben una señal de control para evacuar parte del gas y descender. Lo cual es una característica interesante para vigilancia 7/24.

Por último indicar que pueden transportar un amplio abanico de sensores debido a su capacidad de carga: radares de vigilancia aérea o superficial, sensores fotoeléctricos, enlaces de comunicaciones, sensores meteorológicos, detectores de químicos, equipos ESM, etc.

Bibliografía

«ATO Airship To Orbit», JP Aerospace. America's OTHER Space Program, en: *www.jpaerospace.com*

Brandreth, E. J., jr.: «Airships: an ideal platform for human or remote sensing in the marine environment», OCEANS 2000 MTS/IEEE *Conference and Exhibition*, volumen 3, pp.1.883-1.885, 2000.

Chander, G.; Coan, M. J. and Scaramuzza, P. L.: «Evaluation and Comparison of the IRS-P6 and the Landsat Sensors», IEEE *Transactions on Geoscience and Remote Sensing*, volumen 46, número 1, pp. 209-221, enero de 2008.

Cambone, S. A.; Krieg, K. J.; Pace, P. and Wells II, L.: *Unmanned Aircraft Systems (UAS) Roadmap, 2005-2030*, Department of Defense, United States of America, 2005.

Catálogo UAV SIVA: Instituto Nacional de Técnica Aeroespacial, página *web: www.inta.es/doc/programasAltaTecnologia/avionesNoTripulados/SIVA_1.pdf*

Hain, J. H. W.: «Lighter-than-air platforms (blimps and aerostats) for oceanographic and atmospheric research and monitoring», OCEANS 2000 MTS/IEEE *Conference and Exhibition*, volumen 3, pp. 1.933-1.936, 2000.

Oberc, J.: «Spying for dummies», *Spectrum*, IEEE , volumen 36, número 11, pp. 62-69, noviembre de 1999.

Tutorial de la compañía Boeing «What is a Satellite?», página *web: www.boeing.com/defense-space/space/bss*

UNMANNED VEHICLE SYSTEMS INTERNATIONAL: página *web: www.uvsinternational.org*

WEZEMAN, S. and QUILLE, G.: *UAVs and UCAVs: Developments in the European Union,* European Parliament, Bruselas, octubre de 2007.

Herramientas informáticas

En este apartado se trata de conseguir definir las tecnologías informáticas de vanguardia para dotar a los sistemas de vigilancia y seguridad transfronteriza de las Fuerzas Armadas y las Fuerzas y Cuerpos de Seguridad del Estado en el medio y largo plazo.

Estos sistemas tienen necesidades de *software* ligeramente diferentes a los del sector comercial debido a lo singular de su misión y entorno. No obstante muchos de los atributos del *software* que son más importantes para el sector comercial son directamente aplicables en el sector de la seguridad transfronteriza. Estos son:

- La facilidad de uso.
- Flexibilidad del diseño.
- Capacidades de personalización.
- El coste o precio.
- La fiabilidad.
- El rendimiento.
- La capacidad de soporte a largo plazo.
- La seguridad.
- La escalabilidad.
- La disponibilidad.
- La vida útil.
- La calidad del servicio y del soporte.
- La reusabilidad.
- La interoperabilidad.

Debido a las reducciones presupuestarias, la evolución tecnológica en este campo establecerá la necesidad del principio económico de la eficiencia; es decir, hacer más por menos dinero. Para poder mejorar el desarrollo *software* de estos sistemas se podrán beneficiar de la utilización de las arquitecturas, metodologías y del *software* de base no militar obteniendo ahorros de coste importantes. Además existen otros beneficios potenciales de la equiparación con productos o procesos no militares, como un tiempo

de entrega menor, una mejora en la calidad y la fiabilidad, una reducción en los riesgos asociados al desarrollo y un sistema de soporte ya implantado.

Los requisitos de los Sistemas de Vigilancia Transfronteriza deberán adaptarse a su entorno particular y a los requisitos de la misión. El coste de fallo es muy alto, por tanto la calidad de estos sistemas, es decir, la fiabilidad y el rendimiento son esenciales.

Además deberá tenerse en cuenta la necesidad de disponer de sistemas de tiempo real o de tiempo cuasi real que eviten perder información crítica que comprometa su operatividad y capacidad de respuesta.

Por ello, la calidad de los desarrollos y al mismo tiempo la optimización del coste va a conducir a la evolución de las herramientas y las tecnologías de información. Se utilizarán arquitecturas de referencia, ofreciendo un marco estable de herramientas y desarrollos donde podamos asegurar la reusabilidad y la calidad del *software* al mismo tiempo.

Dentro de las tecnologías encuadradas en el epígrafe «Herramientas informáticas» en las plataformas de sistemas de vigilancia podemos enumerar:

– Arquitectura Orientada a Servicios (SOA).
– Lenguajes de programación.
– Sistemas operativos.
– Herramientas de desarrollo.
– Sistemas de Presentación Geoespacial Avanzada (GIS).
– Sistemas Expertos de Búsqueda *(Data Mining)*.
– Sistemas de Tratamiento y Proceso de Imágenes.

Arquitectura Orientada a Servicios (SOA)

Un modelo de referencia arquitectural es una descomposición estándar de un problema conocido en partes que resuelven el mismo de modo cooperativo. En general un modelo de referencia divide la funcionalidad de un sistema en una serie de elementos, y describe el flujo de información entre los mismos. Al mismo tiempo presenta un modelo de referencia asociado a los elementos *software* y *hardware* que implementan cooperativamente la funcionalidad definida enlos requisitos operativosy recoge los flujos de información entre ellos.

La utilización de una SOA, es y será el elemento de base para los Sistemas de Vigilancia Transfronteriza, siendo los Servicios *Web (Web Services)*

una de las soluciones tecnológicas con mayores posibilidades de consolidación en el futuro y que junto al concepto NNEC *(NATO Networked Enabled Capability)*, permitirán el despliegue y utilización de estas tecnologías dentro de los Sistemas de Seguridad Transfronteriza.

Esta arquitectura presenta un modelo donde las aplicaciones descansan o son implantadas sobre una serie de servicios (por ejemplo: misiones). Un servicio puede realizar una función discreta o un conjunto de funciones del sistema. También varios servicios pueden utilizarse de manera coordinada para implementar funciones más complejas.

La SOA está planteada para ser capaz de compartir funciones de una manera flexible y amplia, sin un acoplamiento excesivo entre las distintas funciones del sistema.

Lenguajes de programación

Se analizan los lenguajes de programación C/C++, ADA y JAVA o RTJ *(Real Time Java)* desde un punto de vista de cumplir los requisitos de los Sistemas de Seguridad Transfronteriza, donde existe la necesidad dedisponer de sistemas de tiempo real o de tiempo cuasi real que eviten perder información crítica que comprometa su operatividad y capacidad de respuesta.

En los sistemas embebidos donde el tiempo real es irrenunciable, C/C++ son los lenguajes más utilizados y se prevé su uso en estos sistemas.

En los sistemas donde es necesaria la concurrencia y al mismo tiempo valga la redundancia el «tiempo real» dos lenguajes de programación ADA y JAVA contemplan estos requerimientos, pero hay que tener en cuenta que de manera muy diferente.

Concurrencia y tiempo real presentan serias dificultades para los lenguajes. ADA y JAVA aunque soportan ambas características difieren en su filosofía. ADA presenta un modelo de concurrencia que puede ser limitado para cumplir la predictibilidad en las aplicaciones donde se requiere tiempo real en sentido estricto y además es la base de los sistemas de aplicaciones críticas certificados con la DO-178B. Por otro lado JAVA ofrece un modelo de concurrencia que ha sido adaptado para cumplir la predictibilidad en aplicaciones de tiempo real.

JAVA es claramente un lenguaje orientado a objetos y muy eficiente en todas aquellas aplicaciones donde los requerimientos de predictibilidad en las aplicaciones de tiempo real puedan ser flexibilizadas, es decir en los sistemas de tiempo cuasi real.

En los grandes sistemas tiene sentido programar diferentes componentes en diferentes lenguajes por ejemplo la interface de usuario en JAVA y los módulos de tiempo real «rabioso» en ADA; de esta manera obtendremos las ventajas de cada uno de los lenguajes.

Sistemas operativos

El sistema operativo son el conjunto de *programas de software* destinados a realizar las tareas básicas entre las que destaca la administración eficaz de recursos físicos *(hardware)* y lógicos.

Comienza a funcionar al iniciar el equipo, o al iniciar una máquina virtual, y gestiona el *hardware* de la máquina desde los niveles más básicos, brindando una interfaz con el *usuario*.

La utilización del sistema operativo adecuado es una de las decisiones claves para el ahorro de tiempo y dinero. La necesidad o no de condiciones de tiempo real estrictas determina la utilización de las soluciones claramente de tiempo real o la utilización de Sistemas Operativos *Open-Source* como *Linux*.

La necesidad de respuesta en un tiempo totalmente predictible determinará la elección de un sistema operativo en tiempo real puro. Para estas partes del sistema será necesaria la utilización de Sistemas Operativos RTOSes donde los tiempos de respuesta son predecibles frentea interrupciones. Cuando los requisitos no son tan estrictos (sistemas de tiempo cuasi real) los sistemas abiertos como *Linux* pueden ser la elección.

Existen distribuciones específicas del Sistema Operativo *Linux*, en su mayor parte sujetas a licencias comerciales, que incorporan características típicas de un RTOS.

Herramientas de desarrollo

Al margen de las herramientas ligadas a los diferentes lenguajes de programación (ADA, JAVA, etc.), ha irrumpido recientemente en el mercado una categoría de herramientas que permiten un grado de abstracción superior a la hora de modelar el comportamiento de los programas. Se trata de las herramientas de desarrollo dirigidas por el modelo o MDD *(Model-Driven Development)*, que se ajustan a la denominada arquitectura dirigida por modelos MDA *(Model-Driven Architecture)*.

Uno de los principales objetivos de MDA es separar el diseño de la arquitectura y de las tecnologías de construcción, facilitando que el diseño y la arquitectura puedan ser alterados independientemente.

El diseño alberga los requerimientos funcionales (casos de uso) mientras que la arquitectura proporciona la infraestructura a través de la cual se hacen efectivos requerimientos no funcionales como la escalabilidad, fiabilidad o rendimiento

MDA es un acercamiento al diseño de *software*, propuesto y patrocinado por el *Object Managemente Group*. MDA se ha concebido para dar soporte a la ingeniería dirigida a modelos de los sistemas *software*. MDA es una arquitectura que proporciona un conjunto de guías para estructurar especificaciones expresadas como modelos.

Usando la metodología MDA, la funcionalidad del sistema será definida en primer lugar como un modelo independiente de la plataforma PIM *(Platform-Independent Model)* a través de un lenguaje específico para el dominio del que se trate.

El modelo MDA está relacionado con múltiples normas, incluyendo el lenguaje de modelado unificado UML *(Unified Modeling Language)*, específicamente con su versión 2.0, MOF *(Meta-Object Facility)*, XMI (*Metadata Interchange)*, EDOC *(Enterprise Distributed Object Computing)*, SPEM *(Software Process Engineering Metamodel)* y CWM *(Common Warehouse Metamodel)*.

Sistemas de Presentación Geoespacial Avanzados (GIS)

Los SIG o GIS (en su acrónimo inglés) son una integración organizada de *hardware*, *software* y datos geográficos diseñado para capturar, almacenar, manipular, analizar y desplegar en todas sus formas la información geográficamente referenciada con el fin de resolver problemas complejos de planificación y gestión.

Un SIG se define como un conjunto de métodos, herramientas y datos que están diseñados para actuar coordinada y lógicamente para capturar, almacenar, analizar, transformar y presentar toda la información geográfica y de sus atributos con el fin de satisfacer múltiples propósitos. Los SIG constituyen una nueva tecnología que permite gestionar y analizar la información espacial y que surgió como resultado de la necesidad de disponer rápidamente de información para resolver problemas y contestar a preguntas de modo inmediato.

Dentro de los Sistemas de Presentación Geoespacial se deberán incluir los de Gestión Geográfica, Meteorológica y Oceanográfica por su importancia dentro de los Sistemas de Seguridad Transfronteriza

En la actualidad los SIG están teniendo una fuerte implantación en los llamados Servicios Basados en la Localización (LBS) debido al abaratamiento y masificación de la tecnología GPS integrada en dispositivos móviles de consumo (teléfonos móviles, asistencia digital personal y ordenadores portátiles).

Por otro lado el mundo de los SIG ha asistido en los últimos años a una explosión de aplicaciones destinadas a mostrar y editar cartografía en entornos *web* como *Google Maps*, *Microsoft Live Maps*, *www.geosyr.com.ar* u *OpenStreetMap* entre otros. Estos sitios *web* dan al público acceso a enormes cantidades de datos geográficos. Algunos de ellos utilizan *software* que, a través de una API, permiten a los usuarios crear aplicaciones personalizadas.

El desarrollo de Internet y las redes de comunicación, así como el surgimiento de estándares OGC que facilitan la interoperabilidad de los datos espaciales, ha impulsado la tecnología *web mapping*, con el surgimiento de numerosas aplicaciones que permiten la publicación de información geográfica en la *web*. De hecho este tipo de servicios *web mapping* basado en servidores de mapas que se acceden a través del propio navegador han comenzado a adoptar las características más comunes en los SIG tradicionales, lo que ha propiciado que la línea que separa ambos tipos de *software* se difumine cada vez más.

Sistemas Expertos de Búsqueda *(Data Mining)*

La minería de datos DM (*Data Mining*) consiste en la extracción no trivial de *información* que reside de manera implícita en los *datos*. Dicha información era previamente desconocida y podrá resultar útil para algún proceso. En otras palabras, la minería de datos prepara, sondea y explora los datos para sacar la información oculta en ellos.

Bajo el nombre de minería de datos se engloba todo un conjunto de técnicas encaminadas a la extracción de conocimiento procesable, implícito en las *bases de datos*.

Las bases de la minería de datos se encuentran en la *inteligencia artificial* y en el análisis *estadístico*. Mediante los *modelos* extraídos utilizando

técnicas de minería de datos se aborda la solución a problemas de *predicción, clasificación* y *segmentación*.

Minería de datos espacial o DM espacial es utilizado para extraer conocimiento interesante y regular. Sus métodos pueden ser usados para entender los datos espaciales, descubrir relaciones entre datos espaciales y no espaciales, reorganizar los datos en *bases de datos espaciales* y determinar sus características generales de manera simple y concisa.

La DM ha sufrido transformaciones en los últimos años de acuerdo con cambios tecnológicos. Los más importantes aplicables a los sistemas de seguridad son:

- La importancia que han cobrado los datos no estructurados (texto, páginas de Internet, etc.).
- La necesidad de integrar los algoritmos y resultados obtenidos en sistemas operacionales.
- La exigencia de que los procesos funcionen prácticamente en tiempo real.
- Los tiempos de respuesta. El gran volumen de datos que hay que procesar en muchos casos para obtener un modelo válido es un inconveniente; esto implica grandes cantidades de tiempo de proceso y hay problemas que requieren una respuesta en *tiempo real.*

Estos cambios están determinando que al ámbito de los sistemas expertos de búsqueda se incorporen tecnologías novedosas o adaptadas de otros ámbitos, muy notablemente las siguientes:

- *Motores de reglas* basados en motores de inferencia. Estos sistemas permiten que a una base de datos de conocimiento (que puede estar siendo alimentada en tiempo real) se apliquen reglas que faciliten la toma de decisiones. Se ha generalizado el uso de algoritmos derivados de RETE para permitir operar a este tipo de motores de reglas en tiempo cuasi real.
- Sistemas de Procesado de Eventos Complejos, CEP *(Complex Event Processing)*. Estos sistemas permiten correlacionar eventos dispersos (por ejemplo: alertas de sensores de distintos tipos) de cara a identificar amenazas ante las que reaccionar de modo sistemático. Se utilizan ampliamente en el ámbito de la seguridad informática.

Sistemas de Tratamiento y Proceso de Imágenes

Los Sistemas de Tratamiento y Procesado de Imágenes juegan un papel vital en los Sistemas de Seguridad Transfronteriza. Serán los encargados de ayudar a los operadores en sus funciones de detección e identificación de las amenazas.

Desde la capacidad de estabilización de los sistemas en movimiento, la fusión de las imágenes de distintas procedencias, o distintas longitudes de onda (visible, infrarrojo, radar, etc.) los Sistemas de Tratamiento de las Imágenes deben dar respuesta a estas necesidades que requieren los Sistemas de Seguridad.

Estos sistemas están basados en el procesamiento digital de las imágenes mediante un conjunto de de técnicas que se aplican a las imágenes digitales con el objetivo de ser capaces de identificar las amenazas, mejorar la calidad o facilitar la búsqueda de información.

Una característica importante que debe proveer un sistema de detección o monitorización automática es la posibilidad de expresar la posición en coordenadas geográficas de un objeto de interés en la imagen, es decir, geolocalizar el objeto.

El uso del tratamiento de imágenes en secuencias de vídeo tiene un gran interés para aplicaciones de detección y de monitorización, pues permiten confirmar de manera precisa las alarmas en las tareas de detección al observar comportamientos dinámicos en una escena.

Las técnicas para la estabilización de las imágenes en vectores en movimiento (vehículos aéreos o terrestres) así como la fusión de imágenes tomadas desde diferentes vectores mediante procesado digital de las imágenes será una de las líneas de actuación de estas tecnologías.

Las líneas futuras de desarrollo en este campo se centran en el empleo de técnicas basadas en el seguimiento de regiones y modelos del terreno para la estabilización de las imágenes y la geolocalización de los puntos detectados en la imagen.

En cuanto a la evolución de las técnicas de procesado de imagen, cabe mencionar la aplicación de técnicas de estimación de las homografías más robustas (tanto para la estabilización como la localización). También es posible considerar modelos más complejos del terreno o del movimiento de las cámaras para la estabilización y localización.

SOLUCIONES TECNOLÓGICAS

Como se deduce de los capítulos anteriores, el estado actual y futuro de la tecnología ofrece un amplio abanico de soluciones parciales al problema de la vigilancia fronteriza. Diversos tipos de sensores operados desde plataformas también diferentes pueden ofrecer a los operadores de los sistemas varias visiones, distintas e incompletas, del escenario fronterizo. Dar una solución tecnológica global al problema en un entorno geográfico concreto implica necesariamente la integración de distintos sistemas, procesando la información provinente de diferentes sensores de forma que se aprovechen las mejores características de cada uno de ellos. Este procesado en el futuro deberá ser realizado de forma automática que es lo que posibilita la integración de un número de fuentes de información amplio (un operador humano puede hacer fusión de información como mucho de dos sensores que tenga operando de forma simultánea).

Por otra parte, el actual escenario fronterizo viene marcado por la aparición de nuevos riesgos y amenazas para la paz, la estabilidad y la seguridad internacionales. En este sentido es necesario impulsar una auténtica política europea de seguridad y defensa. Las estructuras de mando operativas deberán estar interrelacionadas y ser interoperables. Además deberán permitir la cooperación entre diferentes entes nacionales –Fuerzas y Cuerpos de Seguridad del Estado, Fuerzas Armadas, Sasemar, etc.– y organizaciones internacionales, Organización del Tratado del Atlántico Norte (OTAN), Unión Europea, Organización de Naciones Unidas, etc.

Además, los entornos de actuación de los sistemas de vigilancia y respuesta son en general geográficamente extensos. La clave para una respues-

ta rápida y eficaz es conseguir una superioridad en la información, en un entorno deslocalizado espacialmente, y eso implica la necesidad de que la información esté:

> «Siempre disponible a cualquier nivel de decisión, con independencia del lugar en que se encuentre y con las garantías de seguridad adecuadas»[1].

Los condicionantes anteriores no son exclusivos del problema de la seguridad fronteriza, sino que son compartidos en su totalidad por el escenario estratégico de defensa al que se enfrentan las Fuerzas Armadas. Es en este contexto donde ha surgido el concepto NEC *(Network Enabled Capability)* y cuya filosofía y objetivos básicos pueden extenderse directamente al problema de la seguridad transfronteriza, con la ventaja inherente que esto implica de situar la vigilancia de fronteras en el mismo contexto tecnológico al que tiende el conjunto de las Fuerzas Armadas occidentales.

De una forma simplista, diremos que NEC responde a la necesidad de disponer de sensores y de sistemas de apoyo al mando y unidades de respuesta a las amenazas, interconectados de manera que se aproveche de forma adecuada toda la información disponible, traduciéndose en una mejor y más eficiente actuación por parte de los agentes implicados. La base fundamental sobre la que se sustenta este nuevo concepto, reside en el valor de la información y la superioridad que se puede obtener al disponer de información precisa y relevante en el momento oportuno. Como medio para lograr dicha superioridad, se plantea la conexión en una red común a todas las entidades de interés, que participan de algún modo en las operaciones, de forma que cada elemento usuario pueda generar, conocer, aprovechar y difundir la información que pueda resultar útil en cada instante. Las siglas NEC podrían traducirse al castellano como «capacidad basada en red» y parte de la premisa de que ubicar información e inteligencia en una red, de manera distribuida, accesible universalmente, y con los niveles de seguridad, procesado y formato adecuados a cada entorno operativo proporciona capacidades superiores de respuesta a las amenazas. La figura 1 muestra la idea básica del concepto.

[1] Concepto de Información en Red (NEC) del jefe de Estado Mayor de la Defensa, Estado Mayor de la Defensa, Madrid, 2007.

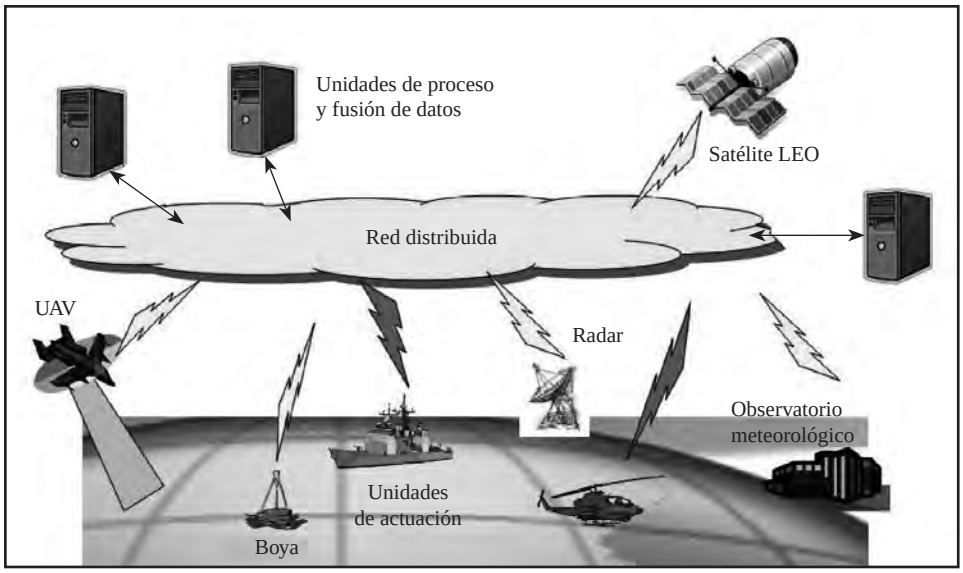

Figura 1.– *Aplicación del concepto NEC a la vigilancia de áreas fronterizas extensas.*

Un aspecto fundamental de esta filosofía son los algoritmos de fusión de información. El tipo de información que generan los diferentes sensores del sistema global es muy diferente y las técnicas de fusión de información deben abordar este reto en los próximos años, ya que hasta ahora la fusión de sensores se ha hecho principalmente sobre sensores de características muy similares. El objetivo final es generar una COP *(Common Operacional Picture)* o lo que es lo mismo, una visión común del entorno de operaciones. Esto no necesariamente significa que todos los agentes implicados deban disponer de la misma información. Significa más bien que aunque todos los actores presentes, puedan disponer de la misma información, únicamente van a extraer aquella que particularmente, le interesa a cada uno, mediante filtros u otros sistemas más avanzados.

La capacidad de integrar todos los componentes del medio operativo (sensores, elementos de decisión y unidades de actuación) desde el nivel político-estratégico hasta el nivel táctico, se sustenta sobre una infraestructura de información y redes. Las características generales que se requerirían son las siguientes:

– Puede concebirse como una «Intranet» gubernamental, multinacional, evolutiva y basada en una federación de sistemas.

– Estará compuesta por sistemas y servicios de comunicaciones e información tanto propietarias como contratadas de forma permanente o eventual.
– Tiene que incluir interfaces de servicios entre distintos cuerpos, organizaciones, naciones OTAN, etc.
– Será una entidad heterogénea y dinámica con constantes cambios de configuración adaptándose al entorno y a los avances tecnológicos.

Para alcanzar los objetivos señalados y lograr cubrir las necesidades operativas, será necesario implantar de forma masiva, tecnologías relativas a las siguientes disciplinas, áreas o familias:

– Arquitecturas Orientadas a Servicios (SOA).
– *Web* semántica.
– Protocolos P2P.
– Técnicas de representación y fusión de la información.
– SCIP *(Secure Communications Interoperability Protocol)*.
– Cifrado con garantías de certificación.
– Redes *black core*.
– *Data Links* diversos.
– Satélites, antenas y conexión inalámbrica, contemplado la cuestión del ancho de banda bajo demanda.
– GPS/*Galileo* integrados en los vectores de comunicaciones y otros.
– SDR *(Software Defined Radio)*.
– EoIP (VoIP, SVoIP y VTCoIP).
– Migración a Ipv6. Cifradores sobre Ipv6.
– Wi-MAX *(Worldwide Interoperability for Microwave Access)*.
– MBWA *(Mobile Broadband Wireless Access)*.
– UWB *(Ultrawide Band)*.
– Mejora de ancho banda de redes y también en comunicaciones inalámbricas.
– Redes móviles definidas y desarrolladas *ad hoc* (MANET,s).
– Modelación y simulación. Metodologías basadas en investigación operativa e inteligencia artificial.
– Nanotecnologías, electrónica de sensores y robótica.

Es evidente que el despliegue tecnológico que exige el concepto es muy ambicioso y en consecuencia es una solución que se prevé operativa en un horizonte temporal de no menos de 10 años.

Quizá una mención especial debe hacerse sobre la tecnología SOA. Las arquitecturas orientadas a servicios, al contrario de las arquitecturas orientado a objetos, están formadas por servicios de aplicación débilmente acoplados y altamente interoperables. Para comunicarse entre sí, estos servicios se basan en una definición formal independiente de la plataforma subyacente y del lenguaje de programación. La definición de la interfaz en cápsula (oculta) las particularidades de una implementación, lo que la hace independiente del fabricante, del lenguaje de programación o de la tecnología de desarrollo. Con esta arquitectura, se pretende que los componentes *software* desarrollados sean muy reutilizables, ya que la interfaz se define siguiendo un estándar, figura 2.

SOA es por una parte una consecuencia del concepto NNEC *(NATO Networked Enabled Capability)*, pero también es la respuesta de la industria a las carencias de integración entre diferentes sistemas, tanto en el mundo civil como en el militar y/o de seguridad. El concepto de las arquitecturas SOA se ha demostrado clave para lograr la interoperabilidad entre diferentes sistemas, como se ha puesto de manifiesto, en diversas

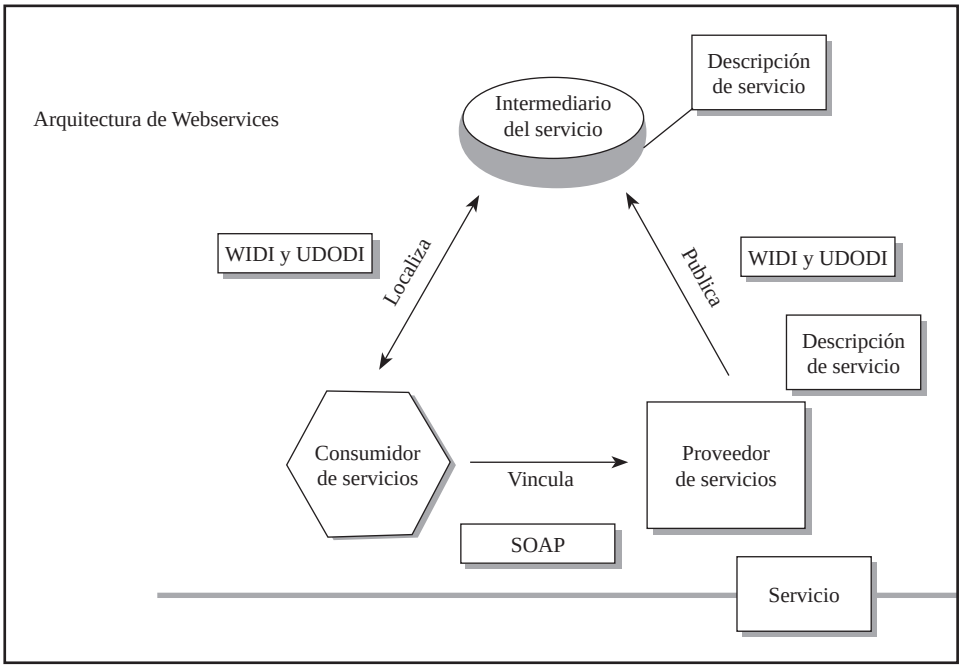

Figura 2.– *Concepto de arquitectura SOA.*

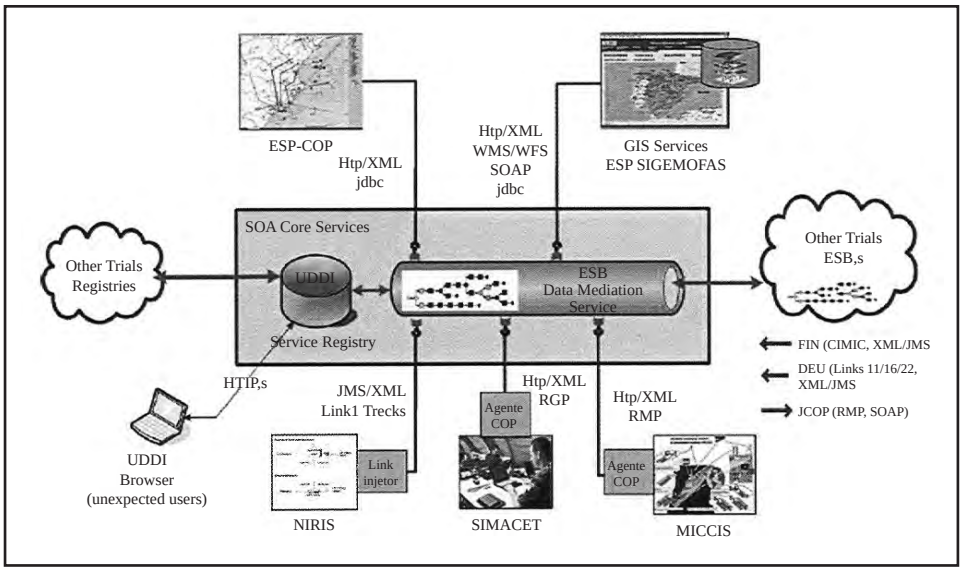

Figura 3.– *Ejemplo de servicios web basados en arquitectura SOA. Participación española de IGECIS en las experiencias CWID 2008.*

experiencias prácticas ya desarrolladas por la OTAN, como por ejemplo CWID 2008, con participación nacional, figura 3.

Finalmente, y para terminar este capítulo, se ha hecho un ejercicio específico de un modelo de sistema que utiliza las arquitecturas tecnológicas descritas y cuyo objetivo primordial sea el de servir de plataforma tecnológica para despliegues diversos, en un entorno marítimo, en los cuales puedan estar implicados diversos usuarios, que aproveche la existencia de sensores y sistemas ya existentes de forma que sea capaz de fusionar toda la información disponible, procesarla para conseguir un escenario operativo unificado con el cual poder realizar procesos de extracción de comportamientos que sirvan a la planificación de las operaciones de los diferentes mandos y usuarios.

Esta figura 4, es válida para un entorno terrestre, en fronteras no reguladas, en donde la plataforma podría integrar sensores de un cuerpo de vigilancia de fronteras, junto a los de policías locales y nacionales, cuerpos de protección civil y servicios sanitarios.

De la misma manera, en el caso de despliegues de las Fuerzas Armadas en misiones en zonas de conflicto, esta solución de integración, permitiría

a nuestras fuerzas obtener información operativa de los sensores de fuerzas amigas, integradas con los sensores propios para poder coordinar las misiones asignadas.

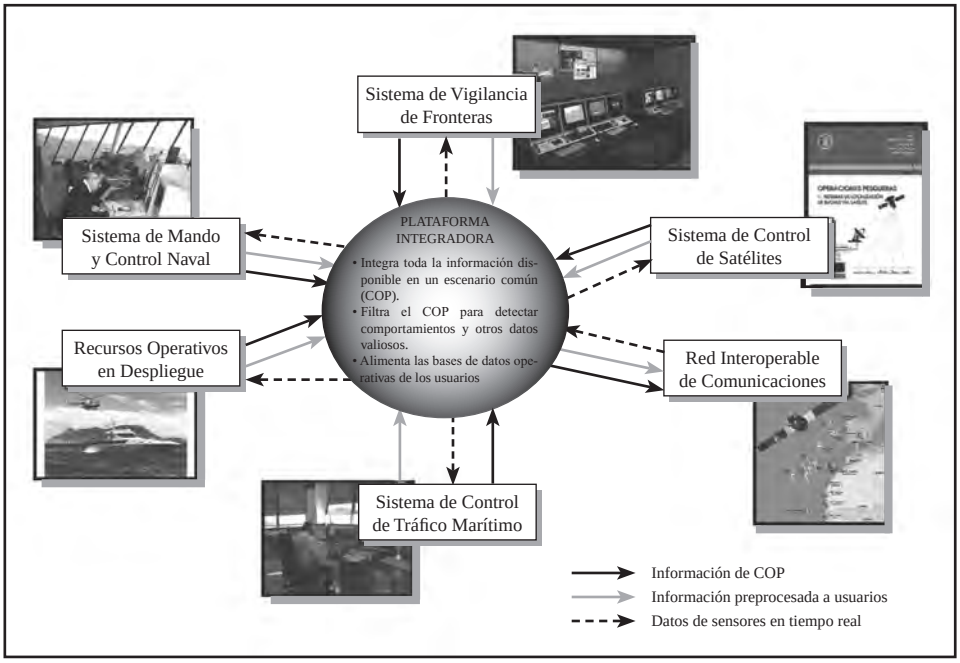

Figura 4.– *Entorno terrestre en fronteras no reguladas.*

VIABILIDAD DEL TEJIDO TECNOLÓGICO

La universidad es sin duda uno de los agentes principales de la Investigación y Desarrollo (I+D) nacional. Valga por ejemplo decir que de los 2.200 millones de euros de presupuesto global para universidades en el año 2008, 500 provinieron del Plan Nacional de I+D. A su vez un porcentaje creciente de la financiación de la investigación en la universidad proviene del sector privado, si bien este porcentaje es todavía muy pequeño (4% en el año 2008).

La capacidad investigadora de la universidad ha experimentado un crecimiento extraordinario en los últimos años a tenor de los indicadores que habitualmente se manejan y basados casi exclusivamente en la producción de publicaciones científicas. Sin embargo, la colaboración con el sector industrial es mínima. Esto a nuestro juicio es un grave defecto de la política científica realizada, y tiene como consecuencia el que el fuerte esfuerzo presupuestario de la I+D revierte muy poco en la mejora del bienestar social a través de la creación de riqueza.

Existen afortunadamente centros y departamentos universitarios que saliéndose de esta norma exhiben una amplia y fructífera trayectoria de colaboración universidad-empresa demostrando la viabilidad y la fortaleza de esta sinergia. Claramente la política científica debe ir orientada a fomentar este tipo de actividad. Y la forma de lograrlo es sin duda a través de los mecanismos de promoción del personal investigador, ligados hasta ahora a la producción científica y que han sido la causa de su espectacular crecimiento. Una política de incentivación y promoción de las actividades de I+D aplicada y en colaboración con la industria representarían sin duda una indicación de madurez del estamento investigador nacional.

Para que esta política tuviera éxito debería de estar complementada con la utilización del tejido industrial tecnológico español de una manera amplia, evitando la excesiva concentración en las grandes empresas que obvian la utilización de empresas pequeñas y medianas. En bastantes ocasiones, las Pequeñas y Medianas Empresas (PYME) son producto de iniciativas de pequeños grupos de emprendedores, imaginativos y muy preparados técnicamente y con una buena experiencia de I+D anterior, capaces de desarrollar productos muy competitivos en plazos muy cortos. El potencial de estas empresas no está siendo utilizado de forma efectiva para el tejido industrial tecnológico nacional. Y es por ello, que sería recomendable la constitución de grupos de interés, coordinados por una gran empresa para constituir equipos altamente especializados capaces de acometer proyectos complejos.

Estos grupos de interés deberían de coordinarse con la universidad y con los responsables operativos de las Fuerzas Armadas y de las Fuerzas y Cuerpos de Seguridad del Estado (FCSE) para conseguir optimizar el esquema de trabajo que se ilustra en la figura 1.

Esta figura sería el deseable a implementar para conseguir que nuestro país consiga las capacidades requeridas, que se han identificado en apartados anteriores y obtener así una superioridad tecnológica en la lucha contra las amenazas esperadas.

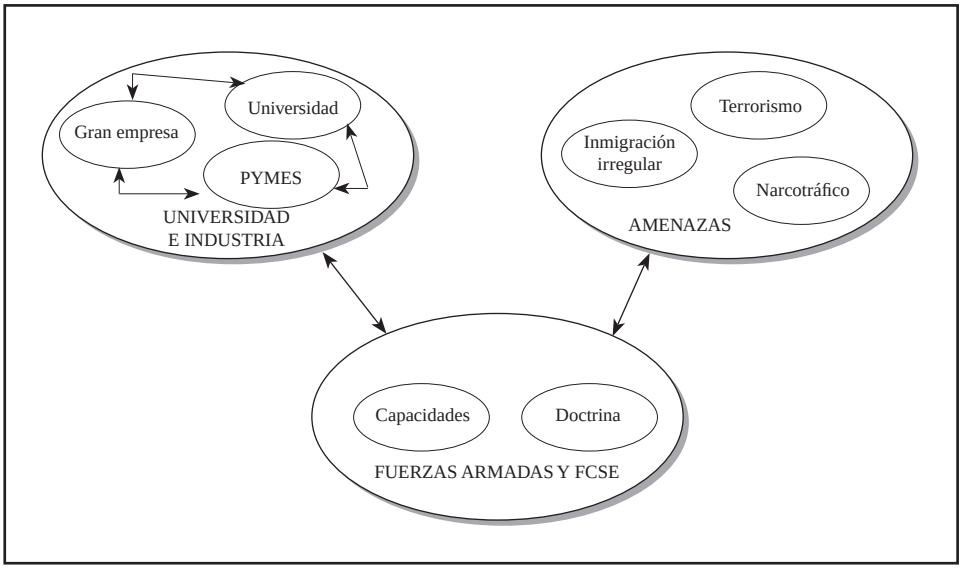

Figura 1.– *Grupos de interés.*

CONCLUSIONES

El objetivo de este *Documento* ha sido el de analizar la problemática de la protección de las fronteras no reguladas en nuestro país y el problema de la autoprotección de nuestras Fuerzas Armadas en operaciones exteriores, desplegadas en territorio hostil o potencialmente hostil, para identificar las capacidades con que se habrían de dotar a las Fuerzas Armadas y a las Fuerzas y Cuerpos de Seguridad del Estado (FCSE) y analizar las tecnologías aplicables, que tratadas adecuadamente connuestro tejido industrial, pudieran proporcionar soluciones a esas capacidades. Y todo ello en un horizonte de los próximos 15-20 años.

Una de las consideraciones más significativas que se han tenido en cuenta en este *Documento* ha sido la nueva visión de la defensa y la seguridad como necesidades interconectadas, frente a la visión clásica de separación entre seguridad como garantía de los derechos y libertades del ciudadano y defensa como protección de los intereses de la nación, que hacen que ambos conceptos hayan de ser tratados de forma integral.

Por otro lado, el análisis de escenarios, riesgos y amenazas a los que nos podemos enfrentar en el horizonte temporal estudiado, arroja variables comunes tanto para la seguridad como para la defensa, reforzando la idea del tratamiento integral.

Como ya vemos en los escenarios de conflictos actuales, las amenazas están y estarán, cada vez, más interrelacionadas. El crimen organizado está claramente interconectado con el terrorismo y con fuerzas militares poco convencionales, lo que los hace más preocupantes, por conseguir sumar las capacidades de una amenaza asimétrica con la potencia de adquisición de capacidades similares a fuerzas armadas de tamaño medio. Estas evidencias, refuerzan la idea del tratamiento integral.

Además, si se revisan los análisis realizados de las tecnologías más adecuadas y de su evolución hacia el escenario futuro, es fácil darse cuenta, que salvo algunas excepciones, estas tecnologías o son de doble uso o se han desarrollado y se están desarrollando bajo un esquema más de tipo civil o si se quiere comercial, en contraposición al esquema clásico de desarrollo de tecnologías para la defensa. Queremos decir con esto, que las tecnologías aplicables a soluciones de sistemas para seguridad, proceden y van a seguir procediendo en su mayoría del mundo civil, o en el mejor de los casos, están siendo desarrolladas como tecnologías de doble uso, pero atendiendo a dar respuesta adecuada a la variable coste-eficacia en la que tanto énfasis se pone en el mundo civil.

Lo que parece evidente, es que de la misma forma que las amenazas han de ser tratadas de forma integral, la constitución de las capacidades también debería de usar un enfoque común, lo que obligaría a las Fuerzas Armadas a aproximarse mas a la utilización de tecnologías de tipo civil como ya se hace por las FCSE. Esto no es un futurible, ya está ocurriendo. Un ejemplo es el Sistema de Información para el Mando y Control del Ejército de Tierra español, ya en fase de renovación tecnológica generacional, y cuya primera fase utilizaba masivamente componentes tecnológicos del mundo civil, adecuadamente robustecidos para su uso en entornos militares.

Además, el propio concepto de tratamiento integral por ambos mundos, conlleva la consecución de un alto grado de interoperabilidad, lo que dirigiría el diseño de los sistemas a soluciones compatibles, que además, podrían redundar en una optimización de los costes de implantación, despliegue, formación y apoyo logístico.

Para conseguir el grado de integración que se propone, faltaría obtener la base tecnológica integrada que se plantea cuando se analiza la problemática del tejido tecnológico español. Sólo una coordinación de los tres actores fundamentales: las Fuerzas Armadas y las FCSE, la universidad y la industria, tal y como se dice en el *Documento*, nos podría permitir la obtención de la superioridad tecnológica que se plantea. Creemos sinceramente que nuestro país tiene tejido tecnológico demostrado para abordar ese objetivo, pero esta herramienta industrial ha de ser utilizada integradamente por las Fuerzas Armadas y las FCSE para poder aprovechar este recurso y conseguir ese posicionamiento que va a ser necesario ante las amenazas y los escenarios futuros que se han descrito en este *Documento*.

COMPOSICIÓN DEL GRUPO DE TRABAJO

Presidente: D. MATÍAS ANEGÓN GARCÍA
Consultor industrial de INDRA.

Secretario: D. CARLOS CORTEJOSO HERNÁNDEZ
Capitán de navío de la Armada y profesor del CESEDEN. EALEDE.

Vocales: D. MATEO BURGOS GARCÍA
Ingeniero de Telecomunicaciones
y profesor titular de la Universidad Politécnica de Madrid.

D. JOSÉ DAVID ALLONA ALBERICH
Ingeniero de Telecomunicaciones y director de la empresa SICONET, S. A.

D. EDUARDO FIGUEROA CUESTA
Comandante de la Guardia Civil, Grupo de Apoyo Operativo.

D. LUIS BÁRCENAS MEDINA
Comandante del Ejército de Tierra, Estado Mayor de la Defensa.

DOCUMENTOS DE SEGURIDAD Y DEFENSA

1. Visión española del África Subsahariana: Seguridad y Defensa.

2. Futuro de Kosovo. Implicaciones para España.

3. Actuación de las Fuerzas Armadas en la consolidación de la paz.

4. El futuro de la OTAN después de Riga.

5. La cooperación militar española con Guinea Ecuatorial.

6. El control de los flujos migratorios hacia España: situación actual y propuestas de actuación.

7. Posible evolución de Afganistán. Papel de la OTAN.

8. Modelo español de Seguridad y Defensa.

9. Posibles escenarios de los *battlegroups* de la Unión Europea.

10. Evolución geopolítica del norte de África: implicaciones para España.

11. La aportación de las Fuerzas Armadas a la Economía Nacional.

12. Reflexiones sobre la evaluación del conflicto de Irlanda del Norte.

13. Fuerzas Armadas y medio ambiente

14. La configuración de las Fuerzas Armadas como entidad única en el nuevo entorno de Seguridad y Defensa.

15. Seguridad y Defensa en Iberoamérica: posibilidades actuales para la cooperación.

16. España y el conflicto del Líbano.

17. La aproximación estratégica a la Europa del Este.

18. La crisis energética y su repercusión en la economía. Seguridad y Defensa Nacional.

19. Seguridad y estabilidad en la cuenca mediterránea.

20. La intervención de las Fuerzas Armadas en el apoyo a catástrofe.

21. Medidas de confianza en el campo de la seguridad en el área euromediterránea.

22. Las Fuerzas Armadas y la legislación tributaria.

23. Dimensión ético-moral de los cuadros de mando de los Ejércitos.

24. Iniciativa norteamericana de misiles y su repercusión en la Seguridad Internacional.

25. Hacia una estrategia de Seguridad Nacional para España.

26. Cambio climático y su repercusión en la Economía, la Seguridad y la Defensa.

27. Respuesta al reto de la proliferación.

28. La seguridad frente a artefactos explosivos.

29. La creación de UNASUR en el marco de la Seguridad y la Defensa.

30. El laberinto paquistaní.