



colegio oficial
ingenieros de telecomunicación

TELECOMUNICACIONES MILITARES PARA EL DESPLIEGUE DE FUERZAS EN MISIONES HUMANITARIAS Y DE MANTENIMIENTO DE LA PAZ

Grupo de Trabajo de Defensa y Seguridad
Colegio Oficial de Ingenieros de Telecomunicación





COLEGIO OFICIAL DE INGENIEROS DE TELECOMUNICACIÓN



colegio oficial
ingenieros de telecomunicación

TELECOMUNICACIONES MILITARES PARA EL DESPLIEGUE DE FUERZAS EN MISIONES HUMANITARIAS Y DE MANTENIMIENTO DE LA PAZ

Grupo de Trabajo de Defensa y Seguridad
Colegio Oficial de Ingenieros de Telecomunicación



Edita: Colegio Oficial de ingenieros de telecomunicación

C/ Almagro, 2 – 1º izda. 28010 Madrid

<http://www.coit.es>

Imprime Langayo www.langayo.es

Depósito legal: M-31041-2013

ISBN: 978-84-936910-2-8



Grupo de Trabajo de Defensa y Seguridad del Colegio Oficial de Ingenieros de Telecomunicación (GTDS-COIT)

Autores:

Juan Manuel Castro Herranz

María del Pilar González-Blanco García

Andrea Iglesias Brocos

Francisco Martin Alonso

María Mateo Iborra

Félix Pérez Martínez

Enrique Rivera del Lucas



PRÓLOGO

Cumpliendo con nuestro deber de servicio público, desde el Colegio Oficial de Ingenieros de Telecomunicación realizamos una labor continua de evaluación y prospectiva sobre los más diversos temas relacionados con las telecomunicaciones y la tecnología, el ámbito de actuación de los profesionales a los que representamos. Un trabajo para el que contamos con los principales expertos que, con total independencia, trabajan para poner al servicio de la sociedad un trabajo riguroso, apegado al máximo a la actualidad y necesidades del país.

En esta ocasión me complace presentar este informe fruto del análisis realizado por los ingenieros de telecomunicación que conforman el Grupo de Trabajo de Seguridad y Defensa del COIT, a quienes agradezco desde aquí su dedicación y esfuerzo, que nos permite, una vez más, cumplir con nuestra función de servir al interés general en nuestro ámbito de competencia. Este grupo, conformado por una representación heterogénea de este sector de altísima especialización (miembros de las Fuerzas Armadas, la Industria, la Universidad y consultoras especializadas) tiene entre sus fines fundacionales promover la cultura de la Defensa y elaborar trabajos que, como este, esperamos sean útiles a las Fuerzas Armadas españolas y a las instituciones y empresas que componen este sector de indudable importancia estratégica.

Las Fuerzas Armadas han sabido utilizar de manera eficiente, los avances tecnológicos para cubrir sus necesidades operativas y, a su vez, conseguir que estas innovaciones impregnen de forma natural su doctrina. El sector de las comunicaciones militares es netamente innovador, y gracias a la dualidad de la tecnología, ha compartido con el ámbito civil muchos de sus más punteros avances, lo que, una vez más, nos obliga a destacar la importancia del establecimiento de políticas e instrumentos que aprovechen las sinergias entre las telecomunicaciones civiles y militares para mantener una industria fuerte que asegure la satisfacción de las necesidades de nuestros ejércitos y sea a la vez fuente de riqueza para España.

“Telecomunicaciones militares para el despliegue de fuerzas en misiones humanitarias y de mantenimiento de la paz” surge porque consideramos que para contribuir al mantenimiento del alto nivel de calidad de la participación de nuestros ejércitos, tanto para las operaciones en el exterior actuales (Operación Reconstrucción de Afganistán, Operación Atalanta en Yibuti, Operación Libre Hidalgo en Líbano, Operación de Apoyo a Mali, etc.) como para aquellas que se desarrollen en el futuro, es conveniente realizar un análisis detallado de los sistemas CIS existentes y los que se prevén en un margen razonable de tiempo. Garantizar la máxima eficacia de la participación española y la seguridad de nuestras tropas en el exterior, pasa sin duda por invertir en este tipo de equipamiento y soluciones, lo que además redundará en una industria nacional fuerte y competitiva.



La evolución de la naturaleza de los conflictos y de los escenarios en que se desarrollan permite atisbar que en los próximos años, perderá fuerza la tradicional idea de Defensa asociada al territorio y concebida para responder a un ataque masivo, incrementándose las misiones no ofensivas, propias de protección civil, reconstrucción y mantenimiento de la paz, en que España ha tenido un importante protagonismo. En este contexto, el dominio de las TIC orientadas a aplicaciones tácticas tendrá una importancia crucial y creciente en las capacidades operativas de nuestras Fuerzas Armadas y vendrá a subrayar la, incuestionada ya, profesionalidad de sus miembros, que garantiza la seguridad de los ciudadanos en un entorno cada día más complejo y globalizado.

Por ello el COIT en este informe ha tratado de realizar un detallado repaso por los principios de funcionamiento, arquitecturas, sistemas y tecnologías que requerirán los modernos ejércitos en sus misiones en escenarios en conflicto. Un trabajo que confiamos sea útil para las Fuerzas Armadas y Cuerpos y Fuerzas de Seguridad del Estado, que vienen asumiendo los nuevos retos tecnológicos con naturalidad y profesionalidad.

Las redes de telecomunicación, como espacio universal de convivencia, requieren prestaciones técnicas cada vez mayores y en este espacio ha de garantizarse también un nivel de seguridad similar al que existe fuera de ellas. Los ingenieros de telecomunicación estamos comprometidos con esta labor y, concretamente, aquellos que día a día desempeñan su trabajo en el ámbito de la seguridad y la defensa. Profesionales motivados y en permanente contacto con las tecnologías más novedosas, que sin duda son un eslabón más en esta cadena de garantías enfocada a reforzar la confianza y seguridad que España necesita y fortalecer su posición internacional.

Eugenio Fontán Oñate.
Decano-Presidente del COIT



RESUMEN EJECUTIVO

La intención de los miembros del Grupo de Trabajo de Defensa y Seguridad del Colegio Oficial de Ingenieros de Telecomunicación (GTDS-COIT) al elaborar este documento ha sido poner de manifiesto la importancia que el dominio de las tecnologías de la información y comunicaciones (TIC) orientadas a las aplicaciones tácticas tendrá en las capacidades operativas de las futuras Fuerzas Armadas, así como aportar al lector una primera aproximación a los principios de funcionamiento, arquitecturas, sistemas y tecnologías que los ejércitos requerirán para llevar a cabo con éxito las operaciones en el exterior que caracterizarán a los actuales y futuros escenarios de conflictos. En sus páginas, además de abordar los aspectos puramente técnicos, también se han analizado las consecuencias de carácter tecnológico, económico y social que de ello se derivan para nuestro país, fundamentalmente los relacionados con la terna ciencia-tecnología-empresa que permitan asegurar que nuestras Fuerzas Armadas puedan disponer de las capacidades necesarias en las zonas de operaciones (ZO) y que estas capacidades puedan ser proporcionadas por la industria nacional –en la mayor medida posible- o la de nuestros aliados.

El documento va dirigido a los miembros de las Fuerzas Armadas, a los profesionales del sector de defensa y a los responsables públicos que tienen que tomar decisiones que condicionan el nivel de operatividad y eficiencia de nuestros efectivos en su participación en operaciones en el exterior en entornos internacionales.

La adecuada obtención y utilización de la información es un factor esencial para asegurar el éxito de las operaciones militares, es lo que se conoce como “Superioridad de la información”, obtenida mediante la aplicación de las tecnologías de la información (TIC). Los medios CIS, de apoyo dentro de la ZO y la conexión con la sede estratégica hasta el más alto nivel de mando, deben ser cuidadosamente planeados antes del despliegue de las fuerzas. Dichos medios deben dotar a los ejércitos de la capacidad de soportar la recolección de información, la evaluación de la situación, la toma de decisiones, la colaboración, la ejecución de la misión y su control.

En este sentido y a partir, entre otras fuentes, de las publicadas en el entorno de la OTAN, en este trabajo se describen las necesidades operativas de las misiones en el exterior y, a partir de éstas, los requisitos para los servicios y las características de las infraestructuras de telecomunicaciones que los pueden suministrar.

La tecnología empleada debe actuar como factor multiplicador de las capacidades operativas; se han identificado las siguientes limitaciones y metas en su uso:



LIMITACIONES	- Disponibilidad de una red adecuada - Herramientas y procesos de gestión de la información/conocimiento - Gran cantidad de datos que desborden a los usuarios - Protocolos de intercambio de la información afectados por restricciones legales, de seguridad o políticas de información - Crecimiento exponencial del número de puntos de fusión de información - Incremento de la presión sobre los combatientes y los sistemas por el masivo intercambio de datos en tiempo real - Vulnerabilidad ante acciones que con tecnologías primarias obstruyen los medios tecnológicamente avanzados. - Cuestionamiento de la seguridad de las operaciones y limitaciones de las mismas por la rápida difusión en los medios de información de datos - Limitaciones en la interoperabilidad de los sistemas CIS en operaciones de cooperación multinacional
METAS	- Apoyo TIC sostenido en ZO - Servicios TIC coherentes e interoperables - Mejoras continuadas en la gestión de los servicios TIC - Flexibilidad y capacidad de respuesta rápida TIC - Dar respuesta a entornos con complejidad creciente

Para afrontar los retos planteados se han identificado los siguientes requisitos como básicos para satisfacer las necesidades de comunicaciones de una red desplegable:

REQUISITOS DE UNA RED DESPLEGABLE	
Para proveer de los servicios básicos de mando y control	- Arquitectura orientada a servicios (SOA) - Seguridad de la Información - Interoperabilidad y dominios de seguridad
Para soportar los servicios de comunicaciones	- Conexión inalámbrica de banda ancha - Gestión eficiente del ancho de banda - Redes de núcleo negro - Calidad de servicio - Cifrado IP - Todo sobre IP - Capacidad "plug and play"

Los requisitos detallados serán implementados en las redes con elementos hardware y software. Para posibilitar la fácil traslación entre requisitos y elementos en los últimos años se ha realizado un gran esfuerzo en formalizar (estandarizar) la representación de la organización de un sistema, es decir, en definir arquitecturas que traduzcan las características de las redes en elementos identificables, que



permitan su adquisición, instalación, integración y posterior gestión y mantenimiento.

En el documento se han identificado una serie de tecnologías clave que conforman los elementos que forman parte de las arquitecturas de las redes desplegables, que son:

TECNOLOGIAS CLAVE

- **Terminales inteligentes y de reducido tamaño, peso, consumo y coste (smart devices, tablet)**
- **Radio cognitiva y SDR, interoperabilidad semántica en formas de onda radio**
- **Gestión dinámica del espectro y nuevas formas de onda (WiMax securizado, LTE securizada)**
- **Redes inalámbricas ad-hoc (MESH, MANET, Redes multisensor)**
- **Sistemas bastionados de identificación y autenticación**
- **Antenas inteligentes y sistemas multisensor**
- **Minería de datos (Data Mining) y Big Data Technologies**

Ya se ha definido qué se necesita pero la cuestión clave es cómo conseguir que nuestras Fuerzas Armadas dispongan de sistemas de información y comunicaciones (CIS) desplegables y que su adquisición genere riqueza y retorno tecnológico a la industria española. La preocupación por la componente tecnológica de nuestros ejércitos la podemos situar con la inclusión en el organigrama del Ministerio de Defensa, desde su creación en el año 1977 (RD 2723/77), de la Dirección General de Armamento y Material que ha liderado la modernización de las Fuerzas Armadas españolas a través de sucesivos programas de I+D+i. En dichos programas se ha hecho partícipe en menor o mayor medida, dependiendo de la complejidad del sistema a desarrollar, a la industria española. El dominio de las tecnologías objeto de este informe es una oportunidad de cara a mantener una industria propia que suministre las capacidades de comunicaciones necesarias a las FAS. En este contexto se identifican los siguientes riesgos y oportunidades para poder desarrollar dichas tecnologías y sistemas:

RIESGOS	- Dependencia tecnológica - Globalización y apertura de mercados - Incremento de la complejidad y coste de los sistemas - Abuso del sistemismo - Política de adquisiciones de “riesgo cero”
OPORTUNIDADES	- Accesibilidad de las tecnologías - Especialización en áreas concretas de actividad - Apoyo de la Administración y en particular del Ministerio de Defensa - Programas de colaboración internacional - Potenciación del mercado exterior - Un idioma y una cultura común - Incremento de la actividad de I+D+i



En los últimos párrafos del documento suponen una primera reflexión y algunas recomendaciones en torno a la importancia de disponer y desarrollar los medios CIS requeridos en las acciones en el exterior por sus sinergias con numerosos sectores de actividad dado el carácter transversal de una tecnologías en rápida evolución –las TIC- que se constituyen en el motor del progreso de las sociedades modernas.

Finalmente indicar que los autores de este documento esperan que su contenido pueda servir de base para la concienciación y habilitación de nuevas líneas de actuación del Ministerio de Defensa, de la Industria española y, en general, del sector de defensa que permitan su beneficio mutuo.



EXECUTIVE SUMMARY

In drafting this document, the members of the Defence and Security Workgroup of the Official Spanish School of Telecommunications Engineers (GTDS-COIT) intend to express the relevance of the operational capabilities of future Armed Forces in mastering Information and Communications Technologies (ICT) geared for tactical applications. This document also intends to provide the reader with a first glance at the operational principles, architectures, systems & technologies that armed forces will require in order to successfully carry out the overseas operations that will set the stage of current and future conflict scenarios. In addition to dealing with strictly technical aspects, this document also analyzes the technological, economic and social consequences that arise for the scientific-technology-corporate triangle in Spain, that allow us to insure that our armed forces will have access to the necessary capabilities within the Operational Zones (OZ), and that said capabilities may be provided by our national industry –to the greatest possible extent- or by that of our allies.

This document is addressed to members of the Armed Forces, defence industry professionals and public authorities that must make decisions that condition the efficiency and operational level of our troops when participating in overseas operations in international environments.

The adequate gathering and use of information is an essential factor towards insuring the success of military operations. This is known as “Information Superiority” which is obtained by applying Information and Communications Technologies (ICT). Prior to the deployment of troops, extensive planning should be performed for Communications & Information Systems (CIS) which provide support within the OZ as well as for the connection to strategic headquarters up to the highest level of command. Such means should provide the armed forces with the capability to support information gathering, situation evaluation, decision making, collaboration and mission control and execution.

To this end, and based, among other sources, on those published within the NATO environment, this text describes the operational needs of overseas operations and from these, the requirements for services and characteristics of the telecommunications infrastructures that can provide them.

The technology used should act as a multiplying factor for operational capabilities; the following limitations and usage goals have been identified:



LIMITATIONS	- Availability of an adequate network - Information/Knowledge management tools and processes - Vast quantities of data that overwhelm users - Information Exchange protocols subject to legal or security restrictions, or information policy - Exponential growth in the number of information processing points. - Increased pressure on combatants and systems due to a massive interchange of information in real time. - Vulnerability to actions that can obstruct technologically advanced means using primitive technology. - Rapid broadcasts of information in the news media which make operational security questionable and limit operations. - Limitations in the interoperability of CIS systems in multinational cooperation operations.
GOALS	- Sustained ICT support within the OZ. - Coherent and interoperable ICT services. - Continuous upgrades of ICT services management. - ICT flexibility and rapid response capability. - Provide answers to environments with increasing complexity.

In taking on the above challenges, the following basic requirements have been identified as essential, in order to meet the communications needs of a deployable network:

DEPLOYABLE NETWORK REQUIREMENTS	
In order to provide basic command and control services	- Service Oriented Architecture (SOA) - Information security - Interoperability and secure domains
For communications services support.	- Wireless broadband connection - Efficient bandwidth management - Black nucleus networks - Service quality - IP encryption - Everything over IP - "Plug and play" capability

The requirements listed shall be implemented with hardware and software elements within the network. In order to allow a smooth transfer from requirements to elements, great efforts have been made during the last few years to formalize (standardize) the graphic representation of the system organization, i.e., in defining architectures that convert network characteristics into identifiable elements that allow their acquisition, installation, integration and subsequent management and maintenance.

This document includes a list of key technologies that make up the elements that are part of the architecture of deployable Networks which are:



KEY TECHNOLOGIES

- Small, lightweight, low power, inexpensive & intelligent terminals (smart devices, tablet)
- Cognitive radio & SDR, semantic interoperability in radio waveforms
- Dynamic spectrum management and new waveforms (secure WiMax, secure LTE)
- Ad-hoc wireless networks (MESH, MANET, Multi-sensor networks)
- Theatre identification and authentication systems
- Intelligent antennas and multi-sensor systems
- Data Mining & Big Data Technologies

We have already defined what is needed but the key issue is how we achieve making deployable Communications and Information Systems (CIS) available to our armed forces while at the same time generating wealth and a technological return for Spanish industry upon its acquisition. We can set a timeframe for the high relevance placed on the technology component of our armed forces which starts in 1977 (Royal Decree 2723/77) with the creation, within the Defence Ministry, of the Weapons and Supplies Department (Dirección General de Armamento y Material), which has spearheaded the modernization of the Spanish Armed Forces through several R&D programs. These programs have included Spanish industry to a greater or lesser degree as a function of the complexity of the systems being developed. Mastering the technologies mentioned in this report is an important opportunity towards establishing a national industry that can supply the communications capabilities needed by the Armed Forces. In this context, the following risks and opportunities in developing these technologies and systems are identified:

RISKS

- Dependence on technology
- Globalization and opening new markets
- Increased system complexity and cost
- Abusive use of system
- “No risk” acquisition policy

OPPORTUNITIES

- Access to technologies
- Specialization in specific areas of expertise
- Support from the Administration, specifically from the Defence Ministry
- International cooperation programs
- Enhance export markets
- A common language and culture
- Increased R&D activity

The final paragraphs of this document offer some thoughts and recommendations relative to the importance of developing CIS systems and making them available as required for overseas operations, while considering their synergies with many sectors and their horizontal nature throughout rapidly evolving technologies –ICT– that form the driving force of progress in modern societies.

Lastly we would like to say that the authors of this document hope that its contents can be the basis for establishing the relevance of CIS Systems within the Defence Ministry, Spanish Industry and the defence sector as a whole, thus leading to new efforts that bring mutual benefits.



Índice

1	INTRODUCCIÓN	19
2	NECESIDADES OPERATIVAS DE LOS EJÉRCITOS Y LA ARMADA EN SUS DESPLIEGUES EN EL EXTERIOR	22
2.1	<i>Escenario Estratégico y Operacional</i>	22
2.2	<i>Características de las operaciones en el exterior</i>	25
2.2.1	<i>Escenarios operacionales</i>	25
2.2.2	<i>Clases de operaciones según conflictos</i>	26
2.2.3	<i>Limitaciones a las operaciones</i>	28
2.2.4	<i>Retos operacionales futuros.....</i>	29
2.3	<i>Requisitos para los servicios básicos de Mando y Control (C2).....</i>	30
2.4	<i>Requisitos para los servicios de comunicaciones.....</i>	33
2.5	<i>Características de las infraestructuras de telecomunicaciones necesarias para misiones en el exterior.....</i>	35
3	ARQUITECTURA DE LAS TELECOMUNICACIONES PARA MISIONES EN EL EXTERIOR.....	37
3.1	<i>Arquitectura de la red troncal de transporte</i>	39
3.2	<i>Arquitecturas de las redes desplegables.....</i>	40
3.3	<i>Arquitecturas de las redes móviles.....</i>	43
3.4	<i>Arquitectura de las redes satélite.....</i>	45
3.5	<i>Arquitecturas de las redes globales</i>	48
4	SISTEMAS DE COMUNICACIONES.....	51
4.1	<i>Sistemas de comunicaciones móviles en bandas HF, VHF y UHF.....</i>	51
4.1.1	<i>Sistemas HF.....</i>	51
4.1.2	<i>Sistemas VHF/UHF</i>	52
4.2	<i>Sistemas inalámbricos de banda ancha.....</i>	52
4.3	<i>Enlaces de datos tácticos.....</i>	54
4.4	<i>Sistemas de comunicaciones por satélite</i>	55
4.5	<i>Otros sistemas.....</i>	57
5	TECNOLOGÍAS CLAVE.....	58
5.1	<i>Terminales inteligentes y de reducido tamaño, peso, consumo y coste (Smart devices, tablets, ...).</i>	58
5.2	<i>Radio cognitiva y SDR, interoperabilidad semántica en formas de onda... ..</i>	59
5.3	<i>Gestión dinámica del espectro y nuevas formas de onda (WiMax securizado, LTE securizado, ...).</i>	61
5.4	<i>Redes inalámbricas ad-hoc (MESH, MANET...)</i>	62
5.5	<i>Sistemas bastionados de Identificación, Autenticación... ..</i>	64
5.6	<i>Antenas inteligentes, sistemas multisensor... ..</i>	66
5.7	<i>Soporte inteligente a las TIC: Minería de Datos (Data Mining), Big Data Technologies... ..</i>	67



6	LAS FUERZAS ARMADAS ESPAÑOLAS ANTE EL RETO DE LAS FUTURAS COMUNICACIONES MILITARES	69
7	EL SECTOR DE LA DEFENSA Y SEGURIDAD ANTE EL RETO DE LAS FUTURAS COMUNICACIONES MILITARES.....	72
7.1	<i>Una oportunidad para la Industria de Defensa en España</i>	<i>72</i>
7.2	<i>Riesgos.....</i>	<i>73</i>
7.3	<i>Oportunidades</i>	<i>76</i>
7.4	<i>Investigación, desarrollo e innovación en telecomunicaciones militares dentro del ámbito de las TIC.....</i>	<i>78</i>
8	CONCLUSIONES Y RECOMENDACIONES.....	81
9	REFERENCIAS	85



Índice de figuras

Figura 1: Telecomunicaciones para el despliegue de Fuerzas expedicionarias OTAN	24
Figura 2: Modelo de escenario de despliegue en Zona de Operaciones.....	25
Figura 3: Topología de red modelo para un escenario de despliegue en ZO	31
Figura 4: Evolución del clásico NEED TO KNOW al nuevo DUTY TO SHARE en IA ..	32
Figura 5: Concepto CIS de jerarquía para interoperabilidad en Zona de Operaciones	33
Figura 6: Anchos de banda comparados necesarios para un despliegue en ZO.....	34
Figura 7: Taxonomía de infraestructuras CIS necesarias para un escenario modelo de ZO	36
Figura 8: Ejes de descripción de una arquitectura de telecomunicaciones	37
Figura 9: Infraestructuras CIS troncales necesarias para un escenario modelo de ZO	39
Figura 10: Infraestructuras CIS desplegables necesarias para un escenario modelo de ZO	40
Figura 11: WiMax táctico	41
Figura 12: Arquitecturas SDR	42
Figura 13: Infraestructuras CIS móviles necesarias para un escenario modelo de ZO	44
Figura 14: Infraestructuras CIS SATCOM necesarias para un escenario modelo de ZO	46
Figura 15: Arquitectura de redes globales	49
Figura 16: Arquitectura del Gestor de Comunicaciones.....	50
Figura 17: Comparativa ENOB vs Ancho de Banda Instantánea	54
Figura 18: JTIDS. Intercambio de información en Link 16.....	55



1 INTRODUCCIÓN

La mayor parte de las acciones militares se pueden describir de forma sencilla como un sistema de sistemas en el que interactúan tres elementos: a) sensores que captan los datos e informaciones procedentes del teatro de operaciones; b) centros o unidades de mando y control que procesan los datos e informaciones disponibles y los convierten en información y conocimiento útil para el desarrollo de la misión; y c) actuadores que ejecutan las acciones necesarias para llevarla a cabo con éxito. Nadie cuestiona que en los futuros conflictos la adecuada obtención y utilización de la información será un factor esencial para asegurar el éxito de las acciones, es lo que se conoce como “superioridad de la información”, obtenida mediante la aplicación intensiva de las Tecnologías de la Información y Comunicaciones (TIC).

En este contexto las Telecomunicaciones, como nexo de unión imprescindible entre los citados elementos, permiten el intercambio de grandes flujos de información y se convierten en un elemento cada día más relevante por su carácter trasversal a todos los elementos y sistemas que participan en un conflicto (mando y control, transporte, sistemas de armas, inteligencia, guerra electrónica...), incrementando su eficacia exponencialmente.

La Telecomunicación se suelen clasificar en estratégicas y tácticas. Las primeras son las que soportan las actividades estructurales de las diferentes fuerzas armadas y se emplean por los mandos militares para definir, dirigir, organizar y emplear las Fuerzas Armadas, tanto en paz, como en los conflictos armados y crisis. Están basadas en enlaces punto a punto por fibra y radioenlaces terrestres, así como en enlaces por satélite. Por el contrario, el objetivo de las comunicaciones tácticas en el intercambio de información entre un gran número de unidades tácticas (plataformas y hombres) desplegadas en un área, en muchos casos muy extensa, que disponen de terminales para la transmisión de voz y datos, con objeto de optimizar las operaciones militares conjuntas. A diferencia de las anteriores, la movilidad es un elemento esencial de estas redes que se emplean fundamentalmente en tiempos de crisis. En algunos ámbitos, también se considera una tercera tipología, las Telecomunicaciones desplegables. Situadas entre las dos anteriores, en ellas no se dispone de la movilidad de las tácticas, pero se pueden desplegar en cualquier escenario por alejado que esté.

El objetivo general de este documento es describir los principios de funcionamiento, arquitecturas y tecnologías de los sistemas de comunicaciones que previsiblemente se requerirán dentro de una decena de años para desplegar las unidades que tengan encomendadas misiones en el exterior. Nos referimos por tanto al conjunto de Telecomunicaciones desplegables y tácticas que se requieren para llevar a cabo misiones de paz o de ayuda humanitaria a zonas en crisis muy alejadas de nuestro país.



La selección de este entorno operativo responde no sólo al hecho de que se trata de uno de los escenarios más previsible para futuras operaciones de nuestras Fuerzas Armadas, tal y como se recoge en la Estrategia Española de Seguridad y la Directiva de Defensa Nacional (ambas a nivel gubernamental), así como en la Revisión Estratégica de la Defensa y en el Libro Blanco de la Defensa (centradas ambas en su correspondiente Departamento), sino también a que los sistemas que las soportarán, por las especiales características de estas misiones, deberán incorporar algunas de las soluciones tecnológicas más avanzadas, que a su vez deberán reflejarse en las futuras versiones de los Documentos anteriormente mencionados. Especial mención debe hacerse a la Ciberseguridad, que dará lugar a un nuevo Documento con entidad propia, la Estrategia Nacional de Ciberseguridad y que no será considerada en estas páginas.

En este documento, además de abordar los aspectos puramente técnicos, también se analizan las consecuencias de carácter tecnológico, económico y social que de ello se derivan, fundamentalmente aquellas relacionadas con las acciones que los diferentes agentes de sistema ciencia-tecnología-empresa deben llevar a cabo para asegurar que las capacidades tecnológicas requeridas estarán al alcance de nuestras Fuerzas Armadas y, en la mayor medida posible, de una industria nacional que garantice –en colaboración con la de otros países aliados- la soberanía tecnológica en este ámbito.

El documento va dirigido a los miembros de las Fuerzas Armadas, a los profesionales del sector y a los responsables públicos que tendrán que tomar en los próximos años decisiones que condicionarán su futuro. La pretensión de sus autores es que sea de utilidad para el mayor porcentaje posible de estos colectivos. Para conseguirlo en ocasiones se ha sacrificado el rigor y la profundidad de la exposición con objeto de facilitar la comprensión de las ideas y conceptos más relevantes incluso para lectores alejados de los temas considerados. Su estructura responde esquema que a continuación se describe:

Tras esta introducción, el segundo capítulo está dedicado a describir las necesidades operativas de las Fuerzas Armadas en el escenario considerado. Así, bajo el título ***“Necesidades operativas de los Ejércitos y la Armada en sus despliegues en el exterior”***, se presentan los escenarios previstos para las futuras misiones conjuntas en el exterior de los tres ejércitos: terrestre, marítimo y aéreo, tanto en el nivel estratégico como en los niveles operacional/conjunto y táctico, aunque serán estos dos últimos los fundamentalmente considerados en este estudio y, por tanto, en los que se han determinado las necesidades operativas en un entorno global y alineadas con las de nuestros aliados.

En el tercer capítulo se describen las arquitecturas generales de los sistemas de comunicaciones que soportarán estas misiones. De este modo con el título de ***“Arquitecturas de telecomunicaciones para misiones en el exterior”***



inevitable se hace referencia al modelo conceptual “Network Enabled Capability” de la OTAN (NNEC) y, de hecho, los conceptos desarrollados en el entorno de esta organización son los elementos básicos incluidos en sus párrafos y han sido los documentos de esta organización los más consultados para redactar este informe.

Los diferentes **“Sistemas de comunicaciones”** que permiten implementar las arquitecturas descritas serán el objeto del siguiente capítulo. Estos sistemas se despliegan en todos los elementos de combate, conectando los centros de mando y control, y permitiendo en intercambio de información entre estos centros y con el resto de elementos, tanto con los sensores que obtienen los datos, como con los actuadores que realizan las acciones para cerrar los ciclos del mando y control.

En el quinto capítulo, **“Tecnologías clave”**, se seleccionan y describen algunas las principales tecnologías que soportan los sistemas de comunicaciones. La selección no es ni mucho menos exhaustiva pues sólo se pretende identificar algunos de los ámbitos tecnológicos más significativos que deben dominarse para poder desarrollar y operar los mencionados sistemas.

A continuación y bajo el epígrafe “Las Fuerzas Armadas españolas ante el reto de las futuras comunicaciones militares” se resumen y aplican las ideas anteriores a la situación particular de nuestro país.

El capítulo séptimo, **“De los centros de I+D a los escenarios de conflicto y los mercados globales”**, está dedicado a reflexionar sobre la necesidad de que el sistema científico-técnico participe en el desarrollo de las tecnologías y sistemas descritas en este informe, con vistas a que las inversiones que inevitablemente habrá que realizar redunden en un valor añadido adicional para nuestro país. En particular se examina el entorno general en que se desenvuelven los distintos agentes, así como las oportunidades y dificultades de nuestra industria nacional para atender a los retos que los mercados globales suponen. La dualidad de las tecnologías implicadas y la trascendencia que ello tiene para asegurar que nuestro país cuente con un sector TIC acorde a su capacidad económica también son objeto de este capítulo.

Finaliza el informe con un conjunto de **“Conclusiones y Recomendaciones”** que resumen el documento insistiendo en la importancia de los sistemas de telecomunicaciones en el mundo militar, la constante necesidad de adaptarlos a los desarrollos tecnológicos asegurando su interoperabilidad con los de nuestros aliados y, por ello, la necesidad de disponer de una estrategia propia para el desarrollo de nuevos productos de alta especialización y eficiencia bajo la premisa de la seguridad nacional.



2 NECESIDADES OPERATIVAS DE LOS EJÉRCITOS Y LA ARMADA EN SUS DESPLIEGUES EN EL EXTERIOR

2.1 Escenario Estratégico y Operacional

El entorno de seguridad actual y futuro, a nivel nacional e internacional, más complejo y menos predecible que en el pasado, requiere de un creciente ritmo de preparación, y de la capacidad de responder rápida y eficazmente a numerosos desafíos, que pueden desencadenarse en forma de efectos en cascada, muy negativos en la seguridad de los Estados. Podemos incluir a título de ejemplo, entre otros, los siguientes:

- El terrorismo transnacional.
- La proliferación de Armas de Destrucción Masiva (WMD).
- La inestabilidad debida a la aparición de Estados fallidos, crisis y conflictos regionales apoyados por ideologías radicales.
- La creciente disponibilidad incontrolada de armamento convencional sofisticado.
- El mal uso de las tecnologías emergentes.
- La interrupción del flujo de los recursos vitales a poblaciones, que genera cambios demográficos y de entorno.
- La seguridad nacional interior y la protección de las fronteras.
- El apoyo a Organismos en las emergencias por catástrofe natural o intencionada.
- La alta disponibilidad de TICs a nivel global, que abaratan los medios de ataque, cruentos o no, e igualan las posibilidades de los adversarios aunque sus diferencias económicas y de medios materiales sean enormes.

Las capacidades NNEC (Capacidades mejoradas en red para OTAN), necesarias obligatoriamente para la consecución del éxito en este tipo de operaciones multinacionales en coalición, orientadas a restablecer el ordenamiento legal allá donde se hubiera descontrolado, con el fin del restablecimiento y mantenimiento de la paz, tomando como base que se producirían conforme a las situaciones entornos antes mencionadas, son las siguientes:



- Enfrentamiento efectivo.
- Superioridad de la información.
- Fuerzas expedicionarias multinacionales.
- Maniobra conjunta.
- CIMIC (Cooperación Cívico-Militar) reforzada.
- Logística integrada.

Asimismo se deben incluir la conexión en una red mundial de sensores, donde se puedan obtener los tomadores de decisiones y los efectores necesarios, dentro de un contexto multinacional, tanto en el ámbito militar y gubernamental como fuera del mismo, dedicados a las actividades de planificación, validación y ejecución de las operaciones.

Las operaciones militares se han reconvertido, de tal modo que se ha pasado de un énfasis en las características cuantitativas de la guerra (masa y volumen) a la comprensión de que los factores cualitativos (oportunidad, indetectabilidad, precisión, sostenibilidad, escalabilidad, acciones y efectos) son facetas cada vez más importantes en las operaciones hoy en día.

Las fuerzas desplegadas, generalmente en colaboración con las de otros países de la OTAN, tendrán que ser de despliegue rápido y sostenible incluso en condiciones adversas, independientemente de la duración y el ritmo de las operaciones requeridas. Para ello es necesario que sean ágiles, conjuntas, combinadas y realmente interoperables en el carácter y el diseño, lo que les permite ser empleadas donde sea y cuando sea necesario. Además, los efectivos militares deben interactuar con entidades fuera de la OTAN, y por lo tanto también se requiere un enfoque más integral a las operaciones.

Los ejercicios previos efectuados con elementos ficticios simulados también proporcionan un alto grado de complejidad que favorece la mejor determinación de la planificación de las operaciones. En el entorno de la Alianza Atlántica, el tamaño y la funcionalidad de los Cuarteles Generales, tanto estáticos como de despliegue, en la Estructura de Mando de la OTAN (NCS), así como de las fuerzas de despliegue nacionales / multinacionales, y de los Cuarteles Generales de la Estructura de Fuerzas de la OTAN (NFS), deben ser adaptados para satisfacer el nivel de ambición (LOA) requerido.

Los servicios C2 (Mando y Control) para las fuerzas desplegadas deben asumir este enfoque y adaptarse en todo momento a las operaciones, con pensamiento y acciones proactivas para lograr ventaja (por ejemplo, física, temporal o condicional) sobre un adversario de muy diversa naturaleza.

La aplicación de un enfoque integral y el desarrollo de NNEC se basan en un fundamento sólido y flexible de los servicios C2. Estos servicios C2 desarrollados en el entorno de la OTAN deben ser reforzados para tener la capacidad de soportar la recolección de información, la evaluación de la situación, la toma de decisiones, la colaboración y la ejecución de la misión y su control.

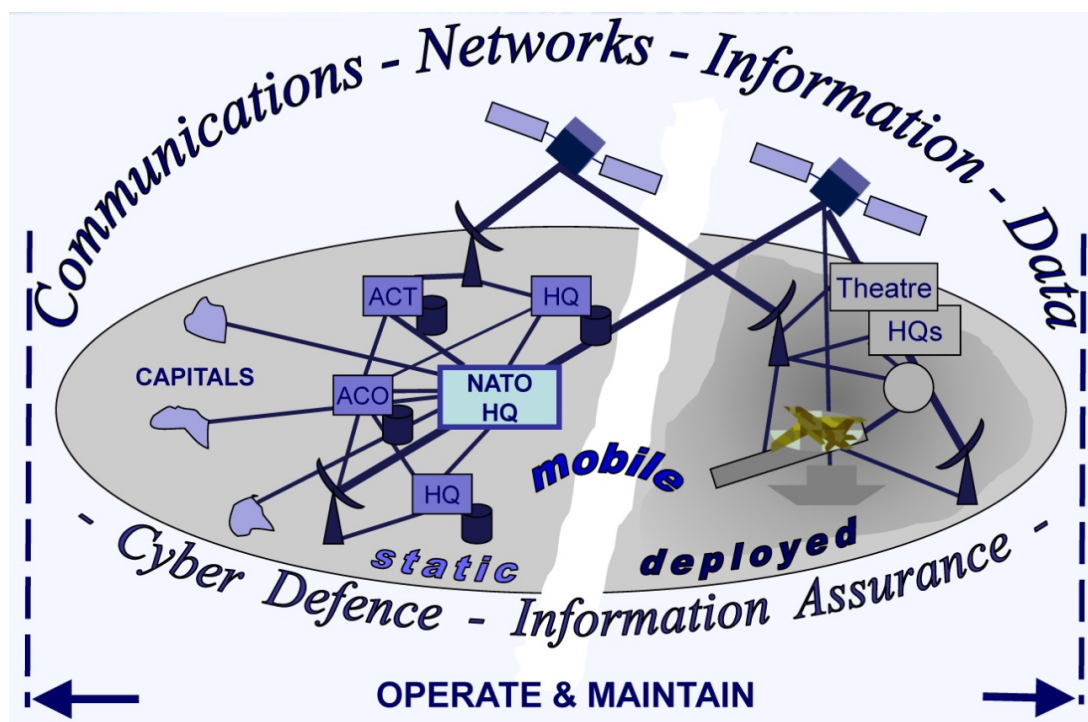


Figura 1: Telecomunicaciones para el despliegue de Fuerzas expedicionarias OTAN

(Fuente: "Secure CIS Services Provision in NATO: Resume and Operational Perspectives", NCSA, Jun 2012)

De esta manera, se facilita a su vez la recepción, la correlación, la fusión y la diseminación de información relevante de múltiples fuentes a los niveles adecuados de mando (desde estratégico hasta táctico). La capacidad de las redes y los sistemas también deben ser conformes a los IERs (requisitos de intercambio de información) de las fuerzas, a través de la transferencia eficiente y la oportuna transferencia de información a través de red apropiada y de la gestión eficiente de ancho de banda.

La interoperabilidad es un elemento crucial en el apoyo al flujo de información, no sólo entre la estructura de mando de la OTAN y sus fuerzas propias, sino también con los Cuarteles Generales de la Estructura de Fuerzas de la OTAN, y por supuesto con las entidades no pertenecientes a la OTAN.

Es por tanto esencial que las fuerzas desplegadas y los elementos que intervienen en las operaciones, realizadas en solitario o en colaboración con otros países de la OTAN, reúnan por lo menos un nivel mínimo acordado previamente y apropiado para sus servicios de C2. La implementación de los servicios C2 en cada nivel de mando de las fuerzas debe ser robusta, segura, fiable, flexible y oportuna, así como la interoperabilidad, para garantizar que estas fuerzas se integran perfectamente en las operaciones conjuntas.



Figura 2: Modelo de escenario de despliegue en Zona de Operaciones

(Fuente: "Software Defined Radio to Enable NNEC: Technical Challenges and Opportunities for NATO"
RTO-MP-IST-083, 2008)

2.2 Características de las operaciones en el exterior

2.2.1 Escenarios operacionales

El espectro de operaciones militares en el ambiente de conflicto descrito anteriormente va desde prevención de crisis a operaciones humanitarias pasando por operaciones de alta intensidad; ello conduce a la necesidad de un tratamiento coordinado en el que intervienen aspectos políticos, militares, civiles y económicos.

Aunque es improbable una agresión en fuerza que lleve a un conflicto de alta intensidad y de tipo bilateral, tal posibilidad no puede rechazarse. Por el contrario, los conflictos asimétricos se sitúan en el terreno de la mayor probabilidad.



Será mucho más probable que, dentro de un concepto multidimensional de seguridad, se den diferentes posibilidades tales como: prevención de conflictos, gestión de crisis, mantenimiento de la paz, imposición de la paz, apoyo a la paz, respuesta a desastres naturales y asistencia humanitaria.

Las operaciones futuras serán más complejas y multidimensionales y las fuerzas deberán adaptarse con rapidez a escenarios cambiantes desde combates letales de alta intensidad a estabilización y operaciones de paz. La obtención, análisis, correlación, discriminación e intercambio de la información será crítica para la anticipación, prevención y contención de los conflictos.

Debemos beneficiarnos de las tecnologías emergentes que nos aseguran mantener la ventaja tecnológica y operativa. La tecnología debe actuar como multiplicador de la potencia de combate. La investigación y desarrollo debe enfocarse en la explotación de la nanotecnología, fuentes de alimentación, espacio, sensores avanzados, sistemas de información y comunicaciones, biotecnología y micro-robótica. Debemos lograr de este modo:

- Apoyo TIC sostenido en zonas de operaciones.
- Servicios TIC coherentes e interoperables.
- Mejoras continuadas en la gestión de los servicios TIC (en su caso).
- Flexibilidad y Capacidad de respuesta rápida en TIC.

Los elementos individuales que comprende la metodología de operaciones basadas en efectos no son nuevos; más bien es un cambio filosófico en el modo de planear y conducir las operaciones. Pone mayor énfasis en la causa y efecto en lugar de la destrucción física de objetivos. Las operaciones basadas en efectos se concretan en alcanzar una situación final estratégica deseada, a través de todas las fases de una operación desde la pre-crisis, pasando por la actividad de alta intensidad, llegando a la de post-conflicto.

2.2.2 Clases de operaciones según conflictos

A continuación se efectúa la clasificación de los escenarios de operaciones prevista en su validez para el periodo 2015-2025. Se dividen los conflictos en tradicionales o convencionales, irregulares o no convencionales, catastróficos, disruptivos (supone utilización de tecnologías avanzadas) y combinación de ellos:

Las **operaciones convencionales** continuarán siendo relevantes en el entorno futuro. Los estados continuaran ligados a estrategias basadas en el uso de fuerzas militares para alcanzar sus objetivos en conflictos pequeños o grandes, en áreas



inesperadas y muy variadas condiciones climáticas y topográficas.

Como demuestran hechos recientes, operaciones a pequeña escala o de estabilización pueden degenerar en hostilidades a gran escala; por tanto, los posibles agresores regionales continuaran modernizando sus fuerzas convencionales e invirtiendo en capacidades que les permitan dominar a sus vecinos.

Simultáneamente, tomando a las posibles coaliciones occidentales como principal amenaza para la consecución de sus ambiciones regionales, estos futuros adversarios adoptarán estrategias contra su acceso al área de crisis.

Los conflictos **irregulares o no convencionales** pueden ser la principal opción de adversarios que son netamente inferiores en fuerzas o tecnología militar; además, pueden unirlos a operaciones convencionales, lo que presenta un escenario incluso más complejo. Actuarán combinando acciones terroristas con emboscadas y combates limitados, incluyendo ataques a autoridades civiles y objetivos no militares. Continuarán desarrollando formas de ataque a las fuerzas terrestres y aéreas, principalmente, con medios y métodos baratos y letales y que impidan el movimiento.

Mediante la protección de sus elementos en terreno difícil y poblaciones y eludiendo enfrentamientos a gran escala para evitar desgaste, el adversario presentará muchas dificultades de identificación y enfrentamiento y se incrementará el riesgo de daño colateral y bajas civiles.

Las operaciones no convencionales se han utilizado a lo largo de la historia y, normalmente no conducen a resultados decisivos para el adversario, pero pueden llevar a un camino sin salida y frustrar la consecución de la estabilidad en el área en cuestión. El éxito en guerra irregular requerirá una serie de medidas coordinadas de distinto signo (militares, políticas, diplomáticas, de ayuda económica, apoyo a la población, etc.).

Los **conflictos catastróficos** incluyen la adquisición, posesión y uso de armas de destrucción masiva (WMD), ataques sobre todo de tipo tecnológico masivo y/o aprovechamiento de catástrofes naturales. Los potenciales adversarios buscan con ellos dominar sus regiones, impedir una intervención exterior, o ambas. La adquisición de WMD por adversarios que no constituyen un estado es una dificultad añadida ya que la decisión de su uso por tales grupos es muy difícil de prever y no puede contrarrestarse con la amenaza de una escalada.

Los conflictos o acciones **disruptivas** se producen mediante el empleo de tecnologías avanzadas que contrarrestan las ventajas que se poseen en algunas áreas operativas clave (ciber-terrorismo, ciberguerra). Los ejércitos deben ser



capaces de hacer frente a esta sorpresa técnica redundando sus sistemas.

El adversario futuro más peligroso será aquel que **combine todas las anteriores acciones**. La introducción de una adecuada sorpresa técnica o la de una modesta capacidad de WMD puede suponer una grave amenaza.

2.2.3 Limitaciones a las operaciones

Existen una serie de factores limitativos para ejercer un adecuado mando y control de las fuerzas militares, entre ellos y como más importantes:

- La disponibilidad de una red adecuada, accesible para todas las fuerzas implicadas. Independientemente de su diseño y capacidad, el propio caos y fricción del campo de batalla influirá en la red diseñada como resultado del esfuerzo operativo, errores, fallos del sistema o acción enemiga deliberada.
- Herramientas y procesos de gestión de la información/conocimiento. No todas las capacidades de la red son necesarias y adecuadas a todos los usuarios en todo tiempo.
- La gran cantidad de datos, información y conocimiento disponible en la red tiene el riesgo potencial de desbordar a los usuarios o limitar el uso completo y adecuado del conocimiento disponible.
- Los protocolos de intercambio de la información pueden verse afectados por restricciones legales, de seguridad o políticas de información.
- El enorme número de puntos de fusión de información, desde el combatiente individual a los futuros sistemas de combate y los órganos de inteligencia correspondientes, incrementan la posibilidad de interpretaciones divergentes de los datos y la información.
- El estrés propio del ritmo elevado de combate y la necesidad de adquirir y procesar datos más rápidamente para tomar decisiones urgentes y acertadas multiplicará la presión sobre los combatientes y los sistemas.
- Los potenciales adversarios encontrarán a menudo capacidades que disminuirán nuestra ventaja tecnológica o recurrirán a acciones que con tecnologías primarias obstruirán los medios tecnológicamente avanzados.
- La rápida diseminación de los reportajes de prensa afectará a la seguridad de las operaciones y establecerá limitaciones en las operaciones.
- La cooperación multinacional es positiva en términos de potencia de



combate, esfuerzo diplomático y capacidades, pero limitativa en términos de interoperabilidad, sobre todo de Sistemas de Información y Comunicaciones (CIS).

2.2.4 Retos operacionales futuros

Las realidades culturales, religiosas, étnicas, políticas y económicas complicarán enormemente el entorno geopolítico futuro. La mezcla resultante de aspectos estratégicos, operacionales y tácticos trasciende las fronteras y proyecta conexiones que presentarán grandes retos y dilemas. Los retos de seguridad serán más variados e impredecibles, el espectro de los conflictos será mucho más complejo, serán más frecuentes las operaciones de estabilidad y en apoyo a la población civil.

Las fuerzas armadas se encontrarán entornos de enorme complejidad física, demográfica y de información. Las alianzas no estarán siempre claras: mientras algunas partes o facciones puedan ser claramente neutrales o amigas, otras pueden apoyar solamente algunas acciones u objetivos de la coalición multinacional correspondiente. Los movimientos estratégicos al área de conflicto envolverán una larga cadena logística de sostenimiento dificultada por la pobre infraestructura de ciertas regiones.

Como ya se ha indicado y a modo de resumen, se pueden postular por tanto cuatros retos de seguridad principales para el futuro: tradicional, irregular, catastrófico y disruptivo. Las operaciones tradicionales o convencionales conducidas en el marco de una disputa estado a estado continuarán siendo relevantes. Los agresores potenciales regionales continuarán modernizando sus fuerzas convencionales e invirtiendo en capacidades que les permitan dominar a sus vecinos. Los conflictos irregulares no convencionales pueden ser la principal elección de antagonistas que son superados en tamaño o en tecnologías militares, o pueden combinar esta clase de operaciones con otras convencionales y presentarán una amenaza incluso más compleja.

Las acciones catastróficas incluyen la adquisición posesión y uso de armas de destrucción masiva. Los potenciales adversarios buscarán estas capacidades para dominar sus áreas regionales, impedir intervenciones externas o ambas. El reto disruptivo puede darse mediante el empleo de tecnologías avanzadas que anulen la ventaja tecnológica existente en coaliciones multinacionales.

El adversario futuro más peligroso será el que combine capacidades de las cuatro formas expuestas. Los oponentes intentarán usar sus capacidades para explotar vulnerabilidades, especialmente la dependencia de los sistemas CIS y más a nivel táctico de los elementos de mando, control, comunicaciones, computación,



inteligencia, vigilancia y reconocimiento (C4ISR).

La característica predominante del futuro es la complejidad: ambientes complejos, enemigos o adversarios complejos y operaciones complejas. Los retos tradicionales requieren métodos avanzados de C4ISR y modernos sistemas CIS para soportarlos. Los retos irregulares requerirán enorme versatilidad y agilidad y posibilidad de detectar modelos de comportamiento muy difíciles de detectar. Las amenazas de catástrofes presentarán retos al planeamiento y preparación de la fuerza y requerirán sistemas flexibles y de respuesta rápida a lo largo de fuerzas muy dispersas. Los retos disruptivos requerirán innovación y adaptabilidad en los sistemas.

La creciente confianza en las alternativas TIC comerciales, unida a los esquemas altamente estructurados de contratación en Organismos nacionales y supranacionales, hacen que debe reconsiderarse a su vez todo el sistema legal que ampara la licitación de cara a la obtención de servicios TIC alquilados a empresas. La deslocalización de dichos servicios a contratar (debido a la globalización empresarial) forzará a ello también de forma natural. El alquiler de capacidad de almacenamiento tipo "cloud", así como la consolidación del creciente ancho de banda serán críticos en el futuro a medio-largo plazo.

El objetivo de los siguientes párrafos de este Informe se centra en el establecimiento de los requisitos exigibles a una arquitectura de comunicaciones que satisfaga las necesidades de un escenario tipo de Zona de Operaciones (ZO) donde se desplieguen Fuerzas multinacionales en coalición, que intentan reducir los efectos causados por las amenazas anteriormente citadas, así como restablecer el orden prefijado por el Derecho Internacional y los Acuerdos Diplomáticos establecidos para tal caso.

2.3 Requisitos para los servicios básicos de Mando y Control (C2)

Se definen a continuación y de manera muy sucinta, los requisitos mínimos de los servicios C2 para las operaciones conjuntas multinacionales, que permiten la colaboración efectiva entre las fuerzas desplegadas, soportados por las infraestructuras de telecomunicaciones necesarias para ello. A continuación se pasará a describir de forma detallada los servicios de comunicaciones mínimos necesarios para garantizar el éxito de las operaciones, conforme a todo lo anteriormente estipulado. Los requisitos mínimos de los servicios C2 se derivan de:

- Conceptos operacionales de alto nivel de la OTAN.

- Lecciones aprendidas / identificadas a partir de anteriores operaciones de la OTAN.
- Resultados de ejercicios realizados por las Fuerzas de Respuesta Rápida (NRF) de la OTAN.
- Consideraciones acerca de la Interoperabilidad.

Los factores clave que determinan el tamaño y el carácter de los servicios C2 para las fuerzas desplegadas en un entorno operativo con base en tierra se describen de la siguiente manera:

C2 de las operaciones de despliegue: La topología de los servicios C2 conforme a la estructura jerárquica de las Fuerzas desplegadas se describe a continuación:

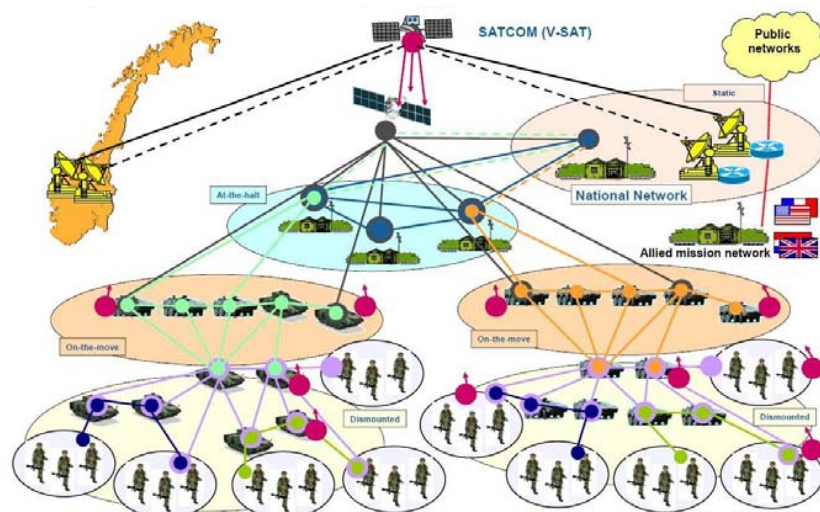


Figura 3: Topología de red modelo para un escenario de despliegue en ZO

(Fuente: "Mobile Deployable Communications" SMi Group, Prague, Feb 2010)

Implicaciones de la Integración de la Tecnología y Evolución de la misma: Las capacidades desplegadas C2 no se pueden quedar demasiado detrás de la tecnología actual, porque la tecnología avanza demasiado rápido. Si ello ocurre, entonces nuestra capacidad de integrar lo que tenemos con las futuras capacidades se hace cada vez más impracticable.

Arquitectura Orientada a Servicios (SOA): La implementación de los servicios C2 en curso deben a los Mandos estratégicos comandos estratégicos y a sus elementos de despliegue, servicios C2 sobre la base de una Arquitectura Orientada a Servicios y de cara al éxito en su enfoque NNEC.

Seguridad de la información (Information Assurance): Operar en un entorno de coalición con entidades de todo tipo, incluso no pertenecientes a la OTAN, convierte en desafiante la infraestructura de las entidades de cara a la seguridad de la información. En NNEC, los mecanismos de seguridad de la información deben estar integrados en todos los aspectos de la arquitectura global, y de este modo operar juntos para lograr el objetivo general de proteger la información, ya sea en reposo o en movimiento. Estos mecanismos ayudarán a asegurar que la información correcta es entregada a la persona adecuada en el momento adecuado, y que la información que reciben es de confianza. El nuevo enfoque de “deber de compartir” equilibrado con el de “necesidad de conocer” clásico expresa esta intención. El deber de compartir requiere que las políticas de seguridad nacionales y de la OTAN junto con procedimientos y sistemas, son desarrollados e implementados con una capacidad inherente para compartir información, pero que implementan las necesarias medidas de seguridad para garantizar que sólo los usuarios autorizados pueden acceder a la información.

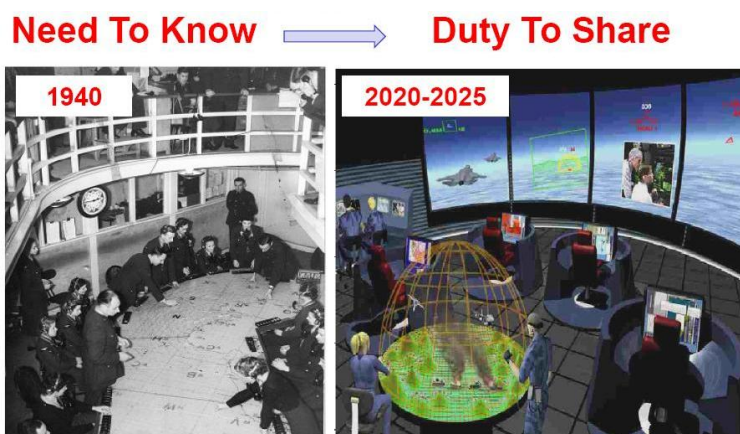


Figura 4: Evolución del clásico NEED TO KNOW al nuevo DUTY TO SHARE en IA

(Fuente: “El Concepto NEC: Aspectos Tecnológicos”, Master en Sistemas de Comunicación para Seguridad y Defensa, ETSIT UPM)

Se impone de este modo la creación de Organismos que se encarguen de la Ciberseguridad o incluso Ciberdefensa de todos los entes implicados, a fin de no solo proteger información clasificada con su acceso sino de garantizar la disponibilidad e integridad de los sistemas de información utilizados, entre otros, para C2.

Interoperabilidad y dominios de seguridad: Con el acuerdo de que NNEC es la meta, el reto para el corto plazo de todas las naciones es ser interoperable con OTAN y entre ellas mismas de forma bilateral. Para ayudar en la consecución de este nivel de interoperabilidad, el concepto CIS (Servicios de Información y Comunicaciones)

para las operaciones de despliegue consiste en conseguir una columna vertebral de comunicaciones OTAN con los receptáculos normalizados de trabajo apropiados para permitir la interconexión entre la OTAN y las Naciones, a nivel de servicio y por medio de pasarelas adecuadas que garanticen la interoperabilidad entre las redes. Esto se representa en la siguiente figura:

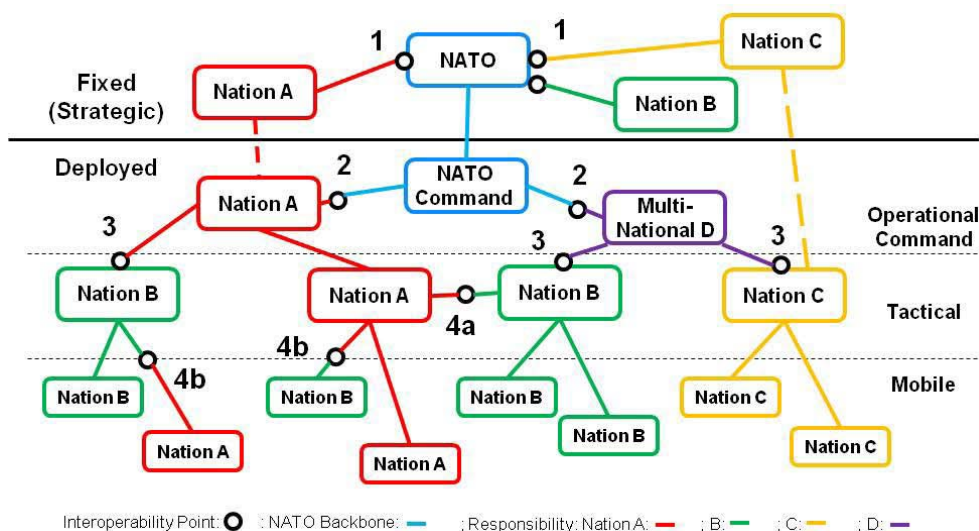


Figura 5: Concepto CIS de jerarquía para interoperabilidad en Zona de Operaciones

(Fuente: NATO C3 Board, Draft MC 0593/1, Jan 2012, "Minimum Level of C2 Services Capabilities In Support Of Joint NATO Operations In A Land Based Environment")

2.4 Requisitos para los servicios de comunicaciones

La capa de Servicios de Comunicaciones se divide en dos, servicios de transmisión y servicios IP. Los servicios de transmisión abarcan áreas tales como las comunicaciones por satélite, servicios inalámbricos, enlaces tácticos de datos y la infraestructura fija cableada. Se identifican las siguientes directrices principales por cada área de la comunicación, que deben existir en todo despliegue en ZO:

Conexión inalámbrica de banda ancha: el uso de formas de onda normalizadas portables. La Radio Definidas por Software (SDR) es vista como un factor clave para establecer formas de onda de cara a la interoperabilidad, y se identifica como la tecnología capaz de conceder la interoperabilidad futura en el campo de batalla.

Redes ad-hoc: la evolución de los protocolos de red permiten la integración en la red IP de los usuarios NNEC con alta movilidad, o en otras redes de aplicaciones específicas (por ejemplo, redes de sensores).

SATCOM: Se describe más adelante con todo nivel de detalle.

Gestión eficiente del ancho de banda: Con el fin de operar totalmente conectados en red, los clientes NNEC, tanto máquinas como seres humanos, tendrán su capacidad de comunicación normalizada en términos de ancho de banda más de lo que tenemos hoy en día. Por lo tanto las redes deben utilizar esquemas de nivel de servicio acordado (SLA) y de gestión de la capacidad asociada.

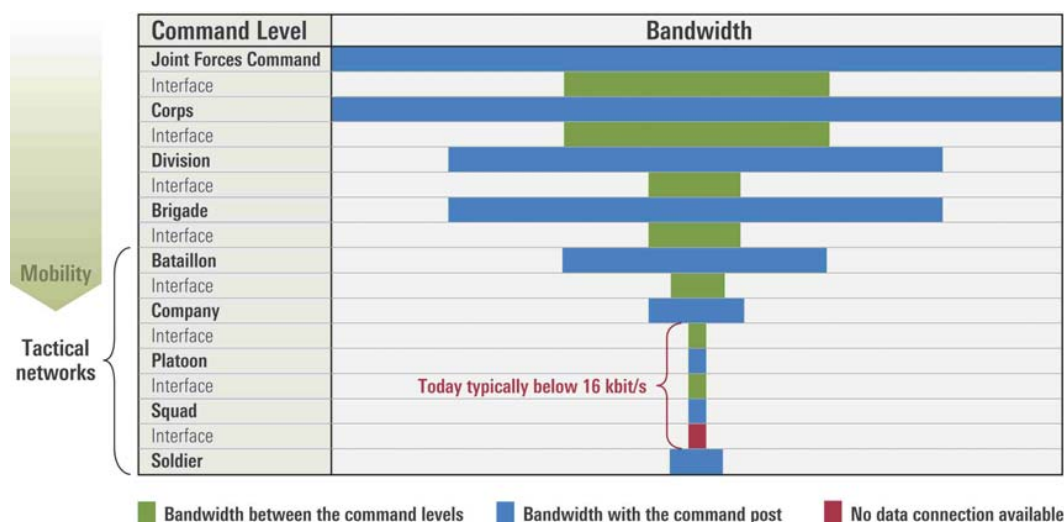


Figura 6: Anchos de banda comparados necesarios para un despliegue en ZO

(Fuente: "International Software Radio 2011: From Software Defined To Cognitive" SMI Group London, Jun 2011)

Redes de Núcleo Negro: Implementación de una red troncal de cara a la seguridad, capaz de soportar el tráfico cifrado y niveles múltiples de seguridad, a través del protocolo IPv6 (IPv4 queda desechado por no permitir el total de las direcciones IP existentes a nivel mundial), y posiblemente alcanzando la federación de más de una "red de núcleo negro". La aplicación de técnicas software de virtualización también permitirán este hecho.

Calidad de servicio: la convergencia de servicios sobre redes IP implica la necesidad de la gestión de calidad de servicio (QoS), de conformidad con los Acuerdos de Nivel de Servicio (SLA) alcanzados con los usuarios de forma previa.

Cifrado IP: Mediante el uso del protocolo IPSEC.

Todo sobre IP (EoIP): La convergencia del tráfico de voz, datos y vídeo sobre IP



que tendrá que ser el mecanismo de transporte común, también deberá ser capaz de satisfacer los requisitos de QoS de las aplicaciones.

Capacidad "Enchufa y Opera": Es decir el apoyo a la movilidad de las unidades operativas que se mueven en la red, que siempre tienen acceso a los servicios que necesitan, sin necesidad de reconfiguraciones manuales.

Servidores proxy: Situados en el borde de la red IP de las Fuerzas de coalición, realizan por ejemplo la tarea de interconexión de redes civiles y militares.

2.5 Características de las infraestructuras de telecomunicaciones necesarias para misiones en el exterior

El despliegue de los sistemas de comunicaciones en ZO implica una transformación de todos los segmentos de las redes e infraestructuras, tanto de acceso como de transporte/troncal, para adaptarlos a las características de la misión. En la figura 7 se presenta la infraestructura CIS necesaria para las misiones consideradas en este trabajo.

Cada servicio de comunicación (ya sea de datos, voz o vídeo), se entregará en los flujos de tráfico IP y se gestionará extremo a extremo por los sistemas adecuados, capaces de optimizar el uso de los recursos de la red en base a la solicitud de usuario, y operar automáticamente efectuando la re-ingeniería necesaria caso de fallos en la red.

La migración de los diversos tipos de tráfico de red a través de un protocolo único, el Protocolo IP, implica la simplificación de la red con claras ventajas en términos de interoperabilidad para redes con tecnologías de transmisión diferentes, el uso óptimo de los recursos, y la reducción de las inversiones. La tecnología clave de esta red será IPv6 que, debido a sus características intrínsecas, parece ser el que va a llevar a cabo la convergencia de todos los servicios a través de un protocolo de red único, resolviendo el problema de la gestión de la calidad de servicio (QoS). La infraestructura de transporte tendrá que poder hacer la gestión de QoS lo más fácil posible, mediante la gestión a su vez del ancho de banda requerido.

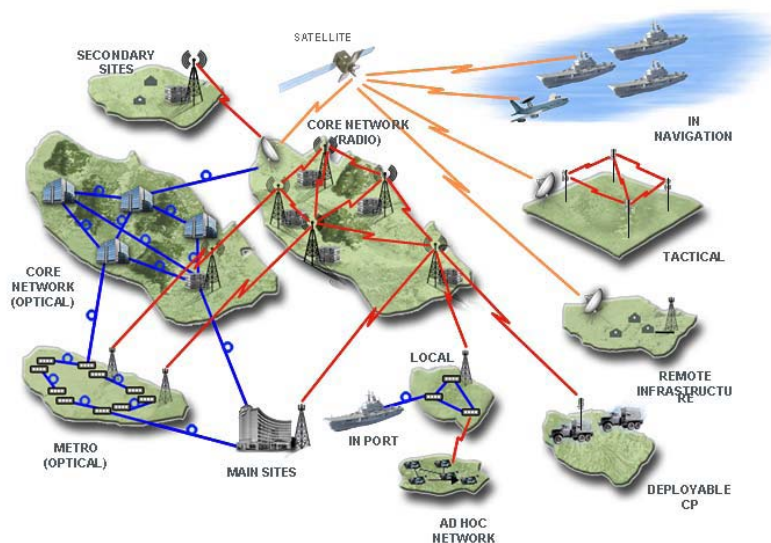


Figura 7: Taxonomía de infraestructuras CIS necesarias para un escenario modelo de ZO

(Fuente: "NATO RTO-TR-IST-067. Annex D – NETWORK EVOLUTION UNDER NNEC CONCEPTS")

Además de tecnologías y protocolos, la arquitectura de la red será de la mayor importancia. La infraestructura de comunicaciones se debe basar en una espina dorsal aportada por las Naciones, de banda ancha, basada en tecnología óptica con elementos de reserva conformados por enlaces por radio en la banda de las microondas, que una las diferentes redes de acceso. De acuerdo a las tendencias destacadas por la OTAN, esta columna vertebral funcionaría como una "red de núcleo negro". Dentro de la red de núcleo negro, tanto de la información clasificada cifrada como no clasificada, se entregarán con una serie de niveles de clasificación, de acuerdo con un sistema de seguridad multinivel.

A continuación se describen con mayor detalle estas infraestructuras.

3 ARQUITECTURA DE LAS TELECOMUNICACIONES PARA MISIONES EN EL EXTERIOR

Generalmente cuando se habla de arquitectura se entiende como la representación de la organización de un sistema o federación de sistemas. Esta organización se representa por sus componentes, sus relaciones entre ellos y con el entorno (interfaces) y los principios que guían su diseño y evolución. Se ha realizado en los últimos años un enorme esfuerzo en formalizar (estandarizar) la manera de describir una arquitectura, con el objetivo de tener un lenguaje común que permita entender la composición y uso de sus elementos en un escenario concreto de forma que este marco sea la vía que permita la interoperabilidad de los sistemas. Entre estas iniciativas podemos relacionar: DoDAF, MoDAF y NAF, cuyo resultado son marcos de referencia de descripción de arquitecturas.

Una arquitectura de telecomunicaciones se puede describir mediante tres ejes, el eje de la funcionalidad o servicios provistos por los sistemas, el eje constructivo o de los componentes e interfaces y el eje del despliegue o de los escenarios de uso (ver figura 8). Este modelo nos provee tres vistas: la vista operativa o vista del usuario final formada por el plano de los ejes de servicios y de despliegue, la vista técnica o constructiva formada por el plano de los ejes de servicios y de componentes y que podríamos denominar la vista del diseñador del sistema y el plano formado por los ejes de componentes y de despliegue que normalmente es la vista de gestión y explotación del sistema.

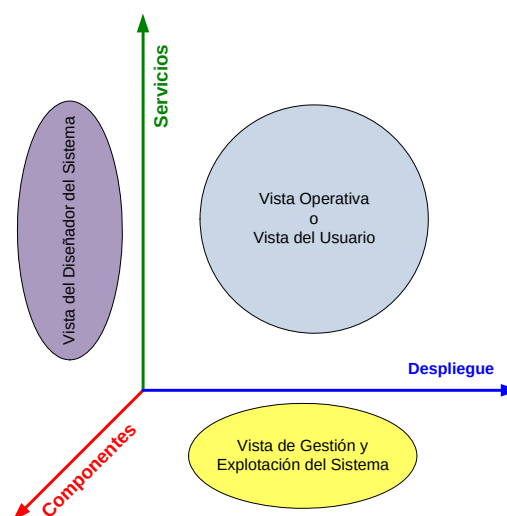


Figura 8: Ejes de descripción de una arquitectura de telecomunicaciones

(Fuente: Elaboración propia)



En el capítulo anterior se ha desarrollado una visión de las vistas de arquitectura correspondientes a los planos operativo y constructivo y en él se mencionan las diferentes soluciones y redes y en que entorno se prevé su uso, quedaría por añadir un resumen de la vista de gestión en la que se trata de ver la arquitectura del sistema desde el punto de vista de sus componentes y despliegue. Esta vista de arquitectura tiene un impacto fundamental en la adquisición y mantenimiento de una solución global de telecomunicaciones. En todo caso hemos de pensar que en el horizonte del que estamos hablando el hincapié se realiza en arquitecturas de redes seguras, que deben cumplir con las necesidades de intercambio de información multimedia de redes de sensores, centros de toma de decisiones y de los sistemas de armas en un ámbito de que abarca los campos táctico, operacional y estratégico y que por tanto deben considerar como parte integrante de estas redes los componentes de comunicaciones de los enlaces de plataformas aéreas y navales ("links") tanto entre ellas, como sus enlaces con los elementos de vigilancia (sensores) y los centros de toma de decisiones.

Para la descripción de estas arquitecturas de despliegue y componentes se utilizan los clásicos conceptos de nodo y enlace, donde aquí nodo se convierte a su vez en varios componentes o sistemas de una ubicación física en un despliegue concreto, y enlace se refiere a una capacidad con una calidad de servicio. Estos nodos, que ya en los diseños actuales poseen una gran complejidad de componentes e interfaces, se conciben con el conjunto de componentes atendiendo fundamentalmente a los siguientes parámetros: servicios a los que dar soporte, ubicación física y movilidad, espacio y consumo. El reto es la definición de las interfaces, no sólo para su conexión con otras posibles redes (redes civiles, otras redes privadas) sino para necesidades futuras. Es decir, la dificultad actual está en proveer y describir correctamente los mecanismos de conexión para la integración en futuras arquitecturas, siendo especialmente sensible los componentes de telecomunicaciones embarcados en plataformas aéreas y terrestres móviles por la escasez de espacio y problemas de alimentación de energía.

Otro elemento fundamental de este plano arquitectural del despliegue es la gestión del espectro y la demanda de ancho de banda. Este punto a su vez lleva a la definición y búsqueda de componentes que, manteniendo las soluciones de arquitectura de despliegue existentes, permitan introducir nuevos componentes/sistemas que, o bien hagan un uso del espectro de forma más eficiente, o bien trabajen en otras bandas de frecuencias menos saturadas.

3.1 Arquitectura de la red troncal de transporte

La infraestructura de transporte actual (figura 9) se basa principalmente en una red troncal de repetidores radio de propiedad gubernamental, junto con enlaces de fibra óptica contratados a operadores comerciales (líneas arrendadas). En cuanto a la evolución a corto plazo del componente de transporte, en los escenarios de evolución se puede identificar:

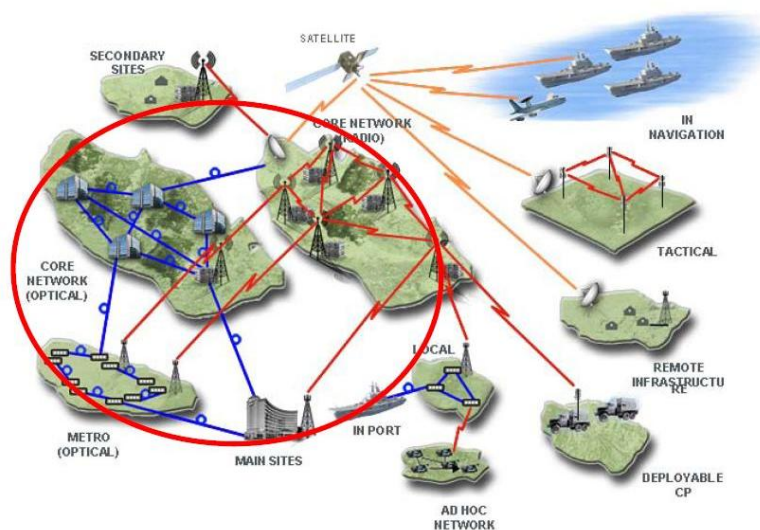


Figura 9: Infraestructuras CIS troncales necesarias para un escenario modelo de ZO

(Fuente: "NATO RTO-TR-IST-067. Annex D – NETWORK EVOLUTION UNDER NNEC CONCEPTS")

- Consolidación de la red troncal nacional de Defensa: Lo deseable es disponer de una infraestructura de transporte integrada capaz de optimizar el uso de los recursos de la red y apoyar todo tipo de servicios de comunicación, incluso los de información sensible o que no es de confianza, con garantía de servicio de extremo a extremo, conforme a petición de los parámetros de información requeridos. La cobertura nacional de la red de transporte debe ser tal que todos los emplazamientos de los usuarios se conectarán, de esta manera reduciendo al mínimo el uso de líneas arrendadas comerciales.
- Incremento del ancho de banda para el usuario: El ancho de banda disponible es un factor crítico para el desarrollo de los sistemas de información. En particular, la disponibilidad para todos los usuarios de servicios colaborativos (audio / vídeo, sistemas de teleconferencia, ...), que requieren una cantidad significativa de ancho de banda, harán que en el futuro aparezca de nuevo un aumento significativo de la carga de tráfico en la red. El aumento de capacidad de transmisión deberá garantizar al menos que se alcanzan algunas decenas de Gbps en toda esta red troncal.

Obviamente la red troncal -generalmente disponible en el propio país- es la que menos modificaciones sufre a la hora del despliegue de una infraestructura de comunicaciones para un país extranjero, sin embargo deberá de adaptarse a las nuevas circunstancias, debiendo de disponer de una flexibilidad y adaptabilidad que asegure que el mando dispondrá de toda la información requerida para la correcta dirección de la misión.

3.2 Arquitecturas de las redes desplegables.

La migración de las funcionalidades de las comunicaciones del segmento desplegable (Figura 10) seguirán las tendencias aplicables a la red troncal, es decir, basarse en el protocolo IP como capa de convergencia, y configurar una "red de núcleo negro" con los dispositivos de seguridad posicionados en el borde del sistema.

Además, las redes de despliegue, actualmente concebidas para cubrir áreas muy amplias con una alta conectividad (denominadas redes "de malla"), evolucionarán a estructuras más ligeras, con menos conectividad jerarquizada de apoyo a Puestos de Mando, y más para actividades operacionales que requieran rápida reconfiguración.

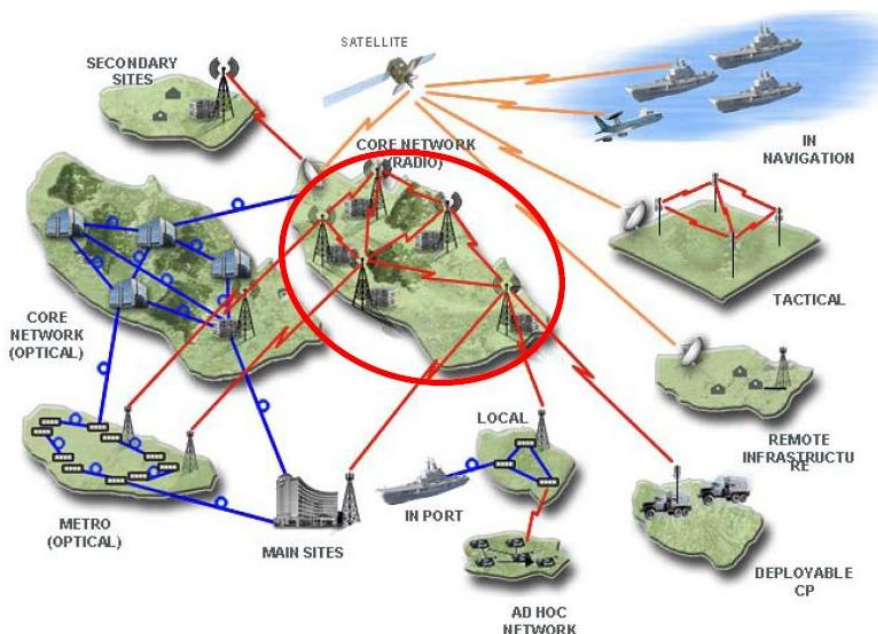


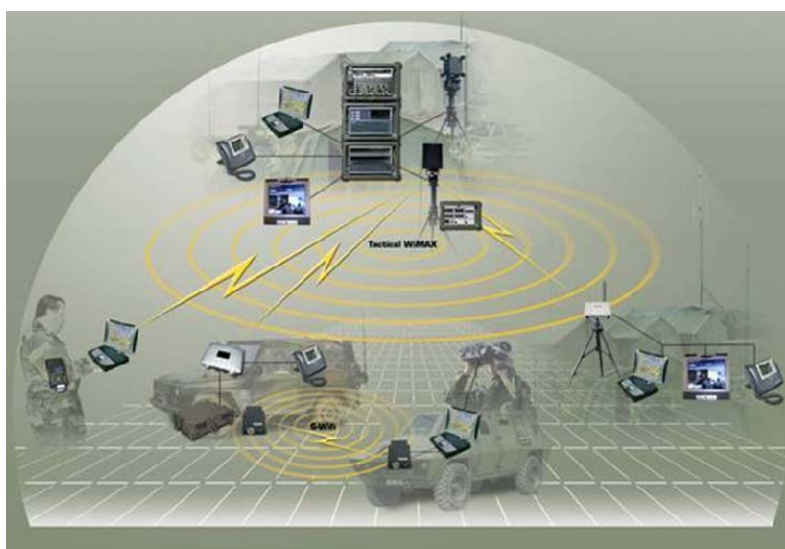
Figura 10: Infraestructuras CIS desplegables necesarias para un escenario modelo de ZO

(Fuente: "NATO RTO-TR-IST-067. Annex D – NETWORK EVOLUTION UNDER NNEC CONCEPTS")

En el caso de los Datalinks (Link-11, Link-16, Link-22) embarcados en aeronaves y buques y que hacen un uso poco eficiente del ancho de banda, existen iniciativas (como la americana WNW o la europea ETAP) que tiene como objetivo el diseño de todo un nuevo sistema desde la forma de onda a los protocolos de red concebidos para dar un servicio de banda ancha.

En el caso de despliegues terrestres se buscan componentes que reduzcan el los elementos de conexión en los puestos de mando desplegados y móviles, sobre todo de cableado, y así se están introduciendo equipos con tecnología tipo WiFi segura ya que ahorran enormemente no sólo el tiempo de puesta a disposición del usuario frente al cable sino aspectos logísticos como el peso y el volumen de los componentes del sistema que hay que desplazar y mantener.

Por otro lado y sobre todo para las operaciones que deben ser llevadas a cabo en vehículos, están apareciendo equipos militares con seguridad añadida al estándar basados en tecnología WiMax para su uso en plataformas vehiculares de comunicaciones y de Puesto de Mando móvil ya que se obtiene la capacidad de funcionamiento en velocidades de hasta 120 Kph con anchos de banda de 30 Mbps y posibilidad de enlaces punto-multipunto. Este tipo de arquitectura es muy interesante para dar conectividad con una reducción muy importante de equipamiento, antenas, peso y consumo de energía así como una más baja huella visual y electromagnética. Se pueden observar en las imágenes ejemplos de vista de arquitectura operacional y de despliegue de un WiMax Táctico (figura 11).



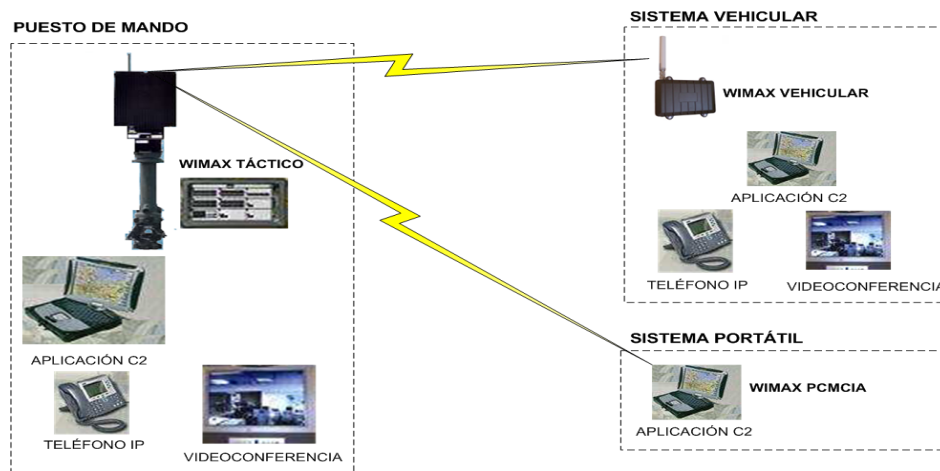


Figura 11: WiMax táctico

(Fuente: Elaboración propia)

La radio definida por software (SDR) con la capacidad de cargar diferentes formas de onda y con diseños de componentes que permitan capacidades multicanal y multibanda dará un nuevo giro al concepto de nodo de comunicaciones táctico actual.



Figura 12: Arquitecturas SDR

(Fuente: Ponencia de Antonio Prieto en la jornada Radio definida por software – SDR de la Fundación
Círculo (17/03/09))



La banda ancha en las conexiones entre los Puestos de Mando en ZO podría ser proporcionado por enlaces tácticos de fibra óptica en el caso de las implementaciones de distancias cortas, o por medio de sistemas inalámbricos en las condiciones de operación en que no se puede permitir el uso de cables de fibra. En este caso, la radio táctica se utilizaría con una capacidad de tráfico máxima en torno a los 40 Mbps, y los sistemas de radiocomunicaciones de banda ancha serían capaces de proporcionar anchos de banda en torno a los 10 Mbps en distancias de cobertura para una gran ciudad (Metropolitan Area Network). La radio táctica desplegable de banda ancha permitirá la comunicación con alta tasa de bits también entre los Puestos de Mando y los usuarios móviles desplegados en los vehículos.

En este ámbito se trabaja en general con tecnología madura y las iniciativas están enfocadas a la mejora del ancho de banda de transmisión y a la no ocupación del espectro radio tradicional, mientras que la introducción de nuevos servicios se orienta más a aquellos que hacen uso de la infraestructura de comunicaciones. No obstante existen una serie de elementos en los que se trata de avanzar como por ejemplo los sistemas MIMO (Multiple Input Multiple Output) con el objetivo de aumentar el ancho de banda de transmisión en los sistemas radio, los componentes en este caso son varias antenas ubicadas en paralelo utilizando cada par de antenas un código CDMA. Por el diseño espacial de este tipo de arquitectura que utiliza como componentes básicos radioenlaces fijos muy direccionales, se minimizan las interferencias mutuas con lo que, para una misma tasa de error, la tasa binaria que se consigue es mayor. Otro ejemplo son los enlaces láser fijos con sus ventajas de moverse fuera del espectro radio y de el gran ancho de banda que ofertan.

3.3 Arquitecturas de las redes móviles

Uno de los retos más apasionantes de NNEC es permitir a un combatiente en ZO, ya sea en vehículo o a pie, tener acceso al mismo conjunto de servicios disponibles en el entorno de la red troncal (figura 13).

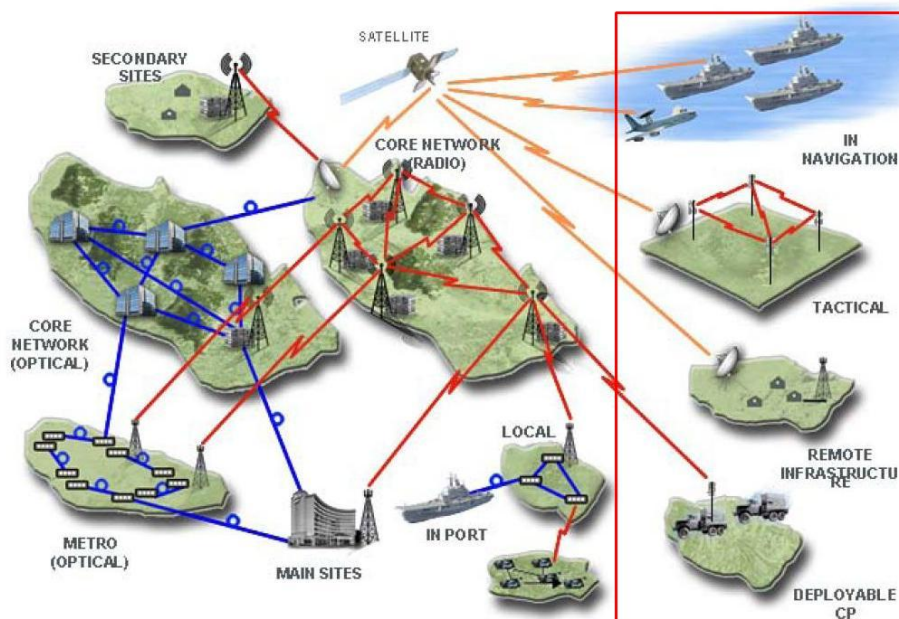


Figura 13: Infraestructuras CIS móviles necesarias para un escenario modelo de ZO

(Fuente: "NATO RTO-TR-IST-067. Annex D – NETWORK EVOLUTION UNDER NNEC CONCEPTS")

Por lo tanto la misma tecnología debe estar presente tanto en las plataformas de vehículos como en esa plataforma especial que es el combatiente junto con su equipamiento. A corto plazo, es necesario aumentar el ancho de banda de transmisión disponible en los vehículos. La introducción de un radio de banda ancha vehicular es la solución que se ha identificado el intercambio de información entre los vehículos, y entre vehículos y emplazamientos de combatientes, en términos de ancho de banda y el uso del protocolo IP. Esta mejora de los sistemas de cara a la movilidad representa el primer paso para lograr las denominadas MANET (Mobile Ad-hoc NETworking ó redes móviles ad-hoc) de alta capacidad.

Desde el punto de vista de esa plataforma que es el combatiente, el primer paso para lograr un soldado con capacidad NNEC pasa por el desarrollo y la implementación del citado concepto, existiendo muchas iniciativas denominadas "Combatiente del Futuro", en diversas naciones aliadas. Se está evaluando la posibilidad de utilizar dispositivos de uso cotidiano tales como "tablets" o "smartphones" en un contexto COTS (Commercial Off-The-Shelf), aprovechando el entrenamiento previo que pueda existir acerca de estos sistemas.

Las comunicaciones tácticas vehiculares y personales serán desarrolladas mediante técnicas de Radio Software Digital (SDR). Se asume que esta tecnología va a conceder las características necesarias esenciales de flexibilidad e interoperabilidad, banda ancha, seguridad y confiabilidad a las comunicaciones móviles en ZO. También será el elemento clave para la extensión de la tecnología IP para el



segmento móvil. Con el despliegue de los sistemas SDR, en el medio plazo se conseguirán las capacidades MANET necesarias para la auto-reconfiguración de los servicios. MANET permitirá, aplicar al nodo vehicular y al nodo de combatiente, las capacidades con el fin de mantener el equipo siempre conectado, entregando en todo momento la posición tanto de vehículos como de combatientes, de forma que también las necesidades del Puesto de Mando se verán facilitadas desde el punto de vista NNEC.

Es por todo ello que la banda ancha inalámbrica va a conferir también la superioridad de la información necesaria en ZO. Los vehículos tendrán que estar equipados con sistemas de radio de banda ancha con características adecuadas para el entorno táctico, tales como la redundancia, la completa conectividad mallada y capacidad de cifrado integrado.

Las comunicaciones de corto alcance (unos cientos de metros), por lo general dentro de un pelotón de combatientes, ó entre combatiente y el vehículo, se realizará por medio de radios digitales de banda ancha también, del tipo portátil de mano, denominado IPR (Radio Individual de Bolsillo), con soluciones adecuadas en el términos de seguridad de las comunicaciones y la fiabilidad. A la espera de la madurez de las soluciones tecnológicas, de nuevo los dispositivos comerciales portátiles tipo “tablet” o “smartphone” dotados de comunicaciones de banda ancha tipo “wi-fi” podrían ser claves en el corto plazo, si bien es necesario identificar una solución para mejorar tanto como sea posible las actuaciones con los sistemas disponibles. El reto a corto-medio plazo también consistirá en como dotar de la seguridad adecuada, para el intercambio de información clasificada incluso, a este tipo de dispositivos móviles que utilizan sistemas operativos novedosos a la vez que flexibles por su naturaleza (Android, Mac, Linux, ...), ya que algunos de ellos son del tipo “software libre”. Los servicios que actualmente están disponibles con la telefonía móvil y la Internet inalámbrica hacen de efecto multiplicador en el campo táctico donde la movilidad, el ancho de banda para la implementación del concepto NNEC y sus servicios asociados, el alcance y seguridad de las comunicaciones, se muestran críticos frente a las soluciones actuales.

3.4 Arquitectura de las redes satélite

El objetivo a largo plazo para esta infraestructura (figura 14) es una completa red IP de banda ancha con QoS SATCOM gestión. Será posible para soportar el aumento de la capacidad de ancho de banda, mediante el uso del rango de frecuencias en Ka y EHF bandas, así como las clásicas en SHF (X y Ku). Esta red tendrá que ser capaz de soportar capacidades de SATCOM en movimiento (SOTM) con terminales satélite compactos.

En efecto, todo apunta a que el futuro de las comunicaciones por satélite está en la banda de frecuencias EHF (Extremely High Frequency), tanto por temas de saturación de frecuencias en las bandas inferiores (SHF/UHF) como por la disponibilidad de un mayor ancho de banda de transmisión, y un menor tamaño de las antenas. Esta tecnología al ser más complicada hace que su puesta en marcha y explotación sea de alto coste por lo que sus primeras aplicaciones son de uso gubernamental y militar. La OTAN ya ha comenzado el proceso de estandarización y ha publicado algunos STANAGS de transmisiones en EHF (por ejemplo el STANAG 4522 y el STANAG 4233). Ya hoy en día los sistemas satélite se utilizan en la mayoría de arquitecturas como redes troncales para dar soporte al enlace entre los campos tácticos, operacional y estratégico. La introducción de componentes con equipamiento trabajando en la banda de EHF mejorará las capacidades respecto a los actuales en cuanto a anchos de banda y tamaño de las antenas.

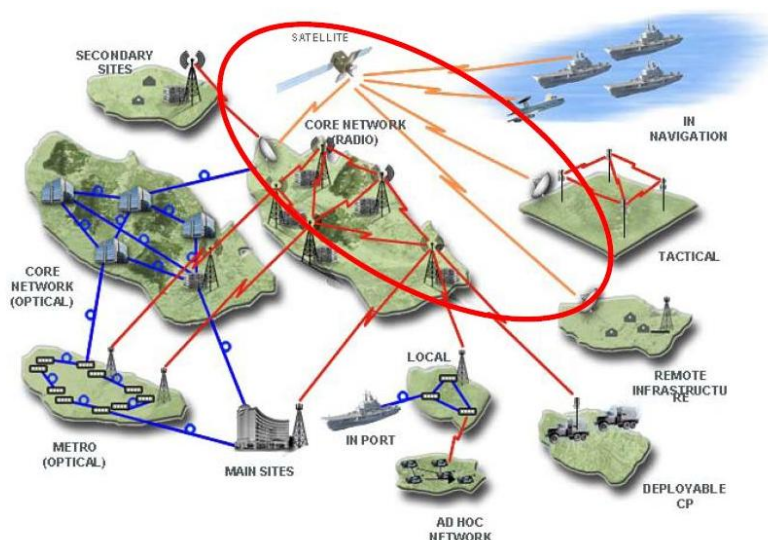


Figura 14: Infraestructuras CIS SATCOM necesarias para un escenario modelo de ZO

(Fuente: “NATO RTO-TR-IST-067. Annex D – NETWORK EVOLUTION UNDER NNEC CONCEPTS”)

En este contexto, aunque no en esta tecnología, también se están produciendo avances importantes en cuanto a la arquitectura de los sistemas haciendo uso de las comunicaciones por láser. La introducción de componentes con equipamiento láser en el diseño de las nuevas arquitecturas se plantea en la arquitectura TCA (Transformational Communications Architecture). En esta arquitectura se prevé el uso de elementos láser para dar soporte a enlaces cruzados entre satélites y



también con plataformas aéreas (aeronaves, UAS's) con anchos de banda de hasta 10 Gbps. Las ventajas del empleo de estos medios tecnológicos están en el gran ancho de banda que proveen, la seguridad que proporcionan, pues la transmisión está basada en haces muy estrechos que en caso de tratar de ser interceptados para su escucha, es fácil de detectar ya que se interrumpiría la comunicación y que no interfieren con los componentes de radiofrecuencia en explotación actualmente. Entre las desventajas nos encontramos con que su uso en la atmósfera, debido a su sensibilidad a las condiciones ambientales tales como humedad, la vegetación, etc. y la necesidad de visión directa entre emisor y receptor limita su aplicación en determinados escenarios fundamentalmente tácticos. Por ello no se plantea en un futuro inmediato su uso en las comunicaciones de los satélites con el segmento terreno.

En el entorno de la red troncal, el satélite tendrá que ser utilizado para:

- Reserva de los enlaces terrestres de alta capacidad.
- Enlace hacia sistemas fuera de la zona de despliegue.
- Conexión de los sitios periféricos situados en ZO, pero a los que no llega la red troncal.

En el entorno de despliegue / móvil, el satélite se utilizará para:

- Una mayor diversificación de las bandas de operación para satisfacer la creciente necesidad de cobertura de las operaciones expedicionarias (concepto NNEC de la agrupación de recursos).
- Para la conexión intra-teatro en ZO de los sistemas de despliegue sin pasar por "hub".
- Para la conexión de los Puestos de Mando móviles ó plataformas navales hacia activos de naturaleza también móvil.

El componente de satélite debe evolucionar en términos de proliferación geográfica, capacidad de despliegue rápido "en movimiento" y las operaciones de gestión de ancho de banda dinámico (con el uso del protocolo IP). Por lo tanto, se prevé la introducción de nuevos sitios "Hub" en la arquitectura de comunicaciones, tanto fijos como desplegables, con el objetivo de descentralizar las funciones de las estaciones de anclaje y la mejora de la recuperación ó reconfiguración de las capacidades.



3.5 Arquitecturas de las redes globales

El salto en las nuevas arquitecturas está en el paso de una situación actual de arquitecturas de red estructuradas en sistemas segmentados, cuya interconexión se realiza por jerarquización, a la posibilidad de “horizontalizar” las comunicaciones. Hasta ahora esto no ha sido posible debido a las dificultades del despliegue y a la concepción de las soluciones en arquitecturas limitadas por el estado de las tecnologías en uso que además no proporcionan el ancho de banda suficiente como para que cualquier nodo de la red pudiese comunicar con cualquier otro. Así mismo tenemos que considerar que los avances en la seguridad multinivel son fundamentales para poder dar el salto a estas arquitecturas de red de concepción horizontal para su uso en entornos de defensa.

Los requisitos de usuario demandan un alto volumen de intercambio, disponibilidad de la información con bajo retardo y aseguramiento de la conectividad. Para ello se necesita un diseño de arquitectura que permita la conectividad lo más directa posible, con redundancia y con gran ancho de banda. El problema del ancho de banda es el de un recurso escaso ya que la demanda supera claramente el disponible, y esta situación se verá penalizada además con la inclusión en red de los sensores. Para disponer del ancho de banda que cubra las necesidades, de nuevo se llega a la conclusión de que hay que suministrar al usuario la capacidad en el momento en que le sea necesario. La solución a este problema pasa por arquitecturas que contemplen diseños con múltiples alternativas, lo que nos lleva a la inclusión de elementos de gestión del ancho de banda distribuidos entre los nodos y los terminales de comunicación del usuario. Esta gestión del ancho de banda pasa por el aprovechamiento de las actuales arquitecturas de red mediante mejoras y el desarrollo de arquitecturas con la concepción de sistemas de sistemas de manera que aparecerán nuevos elementos de enrutamiento, que además puedan ser desplegados de manera móvil (por ejemplo en UAVs o en vehículos) para cubrir las necesidades en diferentes despliegues y en momentos diferentes y con extensión del concepto de calidad de servicio (QOS).

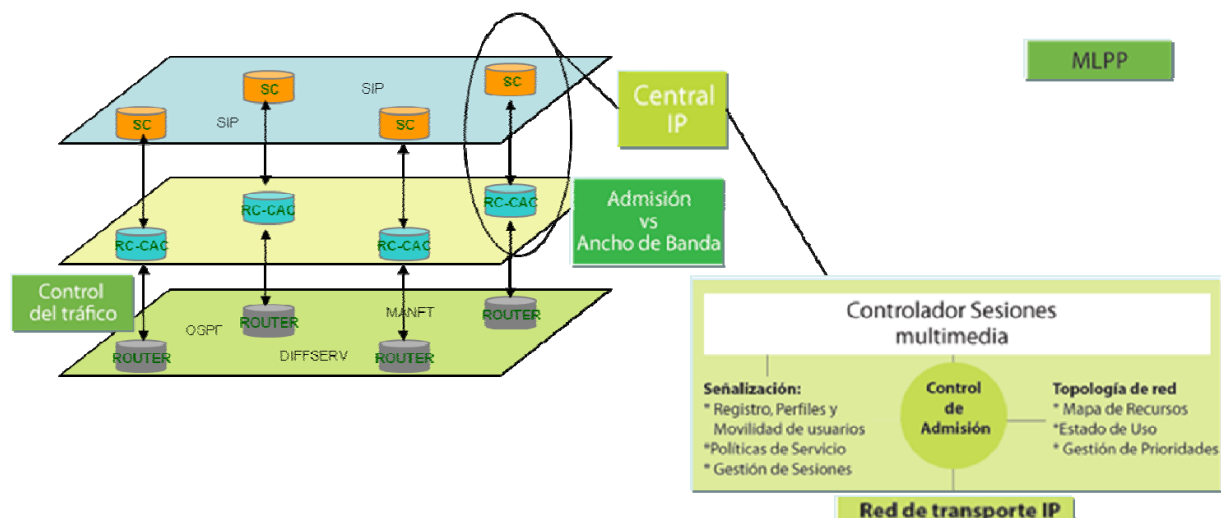


Figura 15: Arquitectura de redes globales

(Fuente: Ponencia de JM Castro de la Jornada "Contribución de los Programas de Armamento y Material del Ejército de Tierra al Planeamiento por Capacidades de la Defensa". Fundación Círculo (25/04/12))

Otro aspecto fundamental que condiciona las arquitecturas de telecomunicaciones viene dado por el espacio de direccionamiento de los protocolos para la identificación de los elementos. La integración masiva de sensores, redes, sistemas de armas, plataformas, y otros elementos de información como los terminales de usuario demandan un gran espacio de direcciones para su identificación. La mayor explotación de los elementos actuales y el diseño que se realiza está basado en una arquitectura de nivel de red basada en un direccionamiento IPv4 que se empieza a demostrar claramente insuficiente tanto por este motivo como por motivos de seguridad. En las nuevas arquitecturas hay que considerar el diseño de los elementos basados en el protocolo IPv6. Este ha sido diseñado para aumentar el espacio de direcciones, mejorar el enrutamiento y la calidad de servicio, facilitar las comunicaciones móviles, proporcionar mecanismos de seguridad extremo a extremo, y simplificar la configuración y gestión de los sistemas. Será además un elemento habilitador para el desarrollo de interfaces entre sistemas diferentes de manera que ampliará la gama de diseños de las arquitecturas actuales. En este caso hay que suponer elementos de integración con capacidades de gestor de comunicaciones entre diferentes medios y equipamientos que permitan proveer una arquitectura de red horizontal. La arquitectura interna de estos elementos debe involucrar tanto las capacidades de enrutamiento como la gestión y seguridad, de manera que se dé una solución de soporte a los diferentes servicios ofertados al lo usuarios independizándolos de los medios de transmisión.

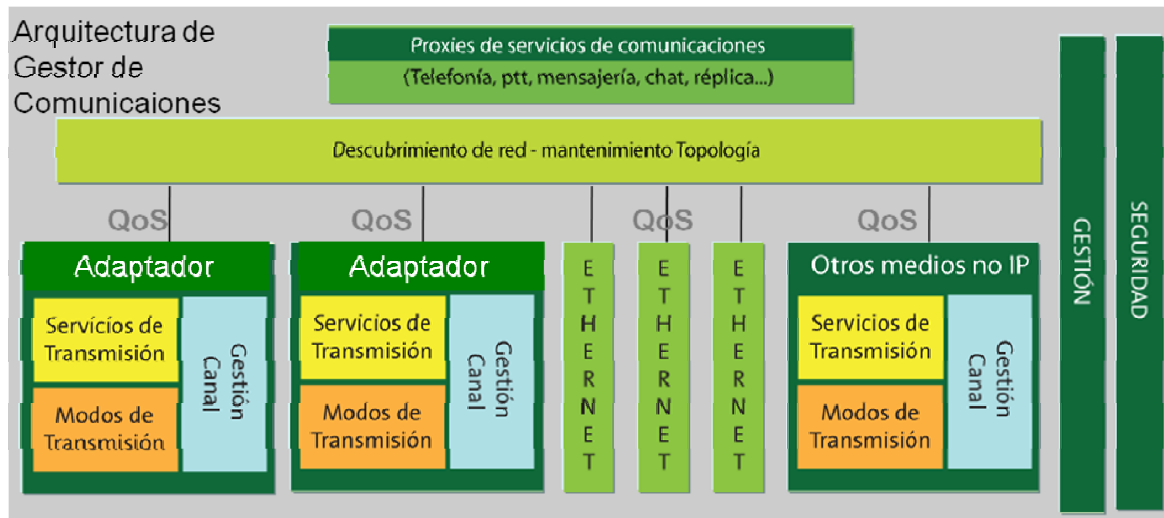


Figura 16: Arquitectura del Gestor de Comunicaciones

(Fuente: Ponencia de JM Castro de la Jornada "Contribución de los Programas de Armamento y Material del Ejército de Tierra al Planeamiento por Capacidades de la Defensa". Fundación Círculo (25/04/12))



4 SISTEMAS DE COMUNICACIONES

4.1 Sistemas de comunicaciones móviles en bandas HF, VHF y UHF

Los sistemas de comunicaciones en las bandas HF, VHF y UHF surgen en los albores de las comunicaciones inalámbricas, cuando existe una aceptación generalizada de que las frecuencias más bajas son mejores para comunicaciones de largo alcance.

Los radioaficionados descubrieron por aquel entonces la capacidad de la banda HF (2 – 30 MHz) para comunicaciones de largo alcance a través de la ionosfera usando sólo modestos transmisores y antenas. En un principio, se pensó que las comunicaciones VHF (30 – 300 MHz) y UHF (300 MHz – 1 GHz) quedarían limitadas a la línea de vista o comunicaciones con visión directa (LOS – Line Of Sight por sus siglas en inglés). Sin embargo, a raíz de la 2ª Guerra Mundial, se descubrieron un número de modos de scattering o dispersión que provocaban que estos sistemas pudieran funcionar de forma satisfactoria más allá de la LOS, lo que provocó su evolución hasta los sistemas utilizados hoy en día.

Entre los sistemas HF/VHF/UHF de Defensa en nuestro país destacamos los nodos permanentes y los nodos desplegables con capacidad CIS de la UME (Unidad Militar de Emergencias).

4.1.1 Sistemas HF

Los sistemas HF ofrecen comunicaciones de larga distancia (llegando a cubrir todo el planeta) a través de la ionosfera. Requieren solamente transmisores y antenas modestos, sin necesidad de infraestructura adicional externa. Los enlaces HF pueden establecerse fácilmente desde localizaciones remotas y también son idóneos por su simplicidad para el despliegue tras un desastre natural.

Sin embargo, dada la naturaleza variable y dispersiva de la ionosfera, este tipo de comunicaciones exige unos requisitos muy estrictos en cuanto a protocolos de comunicación y hardware. Además la frecuencia de transmisión idónea varía mucho dependiendo de diversos factores entre otros manchas o llamaradas solares así como el momento del día (por la noche se pueden usar frecuencias menores de 10 MHz mientras que durante el día esta banda es más complicada de utilizar).

En el ámbito militar, el límite inferior de la banda HF se fija en 100 kHz, no obstante la mayoría de las comunicaciones tienen lugar por encima de los 2 MHz.



4.1.2 Sistemas VHF/UHF

Las características de propagación que proporciona el VHF son ideales para comunicaciones terrestres de corta distancia, con un alcance algo superior a la LOS. A diferencia de los sistemas HF la ionosfera no refleja habitualmente este tipo de ondas así que las transmisiones quedan restringidas a comunicaciones locales, inferiores a 100 millas. Las comunicaciones en VHF son más robustas que las HF frente al ruido atmosférico y las interferencias de equipos eléctricos; sin embargo son más vulnerables frente a características naturales del terreno (colinas, montañas, valles, etc.).

En el caso de los sistemas UHF, dado que estas transmisiones al ser más altas en frecuencia tienen una longitud de onda menor, requieren antenas más pequeñas y menos llamativas. A cambio quedan limitados a comunicaciones más cercanas (por debajo de LOS) y la existencia de edificios u objetos dificulta mucho la comunicación.

En el ámbito de comunicaciones militares, existen sistemas de VHF, UHF e híbridos. Se utilizan para proporcionar comunicaciones tácticas de voz y datos entre los diferentes actores (plataformas y personas) en el escenario de operaciones. Normalmente se trata de unidades compactas y portátiles que se usan para intercambio de información oral, sea en sistemas punto a punto o en sistemas de radiodifusión (broadcast).

Los sistemas VHF/UHF se pueden utilizar en numerosas aplicaciones como seguridad pública, sistemas de emergencia, transportes, etc. En estas frecuencias existen sistemas analógicos, digitales y troncales (trunk) en numerosas frecuencias diferentes, para uso público, privado y militar.

A modo de conclusión cabe afirmar que estas bandas de frecuencia han jugado y jugarán un papel fundamental en las comunicaciones fijas a muy larga distancia (HF) y en las desplegables y tácticas (VHF y UHF), como medio de transmisión esencial por sus características de propagación. Los nuevos desarrollos tecnológicos irán orientados tanto a desplegar sobre ellos nuevas capacidades y servicios como a superar sus actuales limitaciones: congestión del espectro, dependencia de su calidad de las condiciones particulares del entorno y extensión de las acciones de guerra electrónica.

4.2 Sistemas inalámbricos de banda ancha

En los sistemas CIS dentro del ámbito de defensa, los diferentes actores (militares, servicios de emergencia, etc.) deben compartir información vital que puede tener diferente tamaño y formato (voz, imágenes o vídeos, por ejemplo).

Desafortunadamente durante décadas los sistemas de comunicaciones eran poco



fiables e inadecuados. Así constantemente se han llegado a encontrar situaciones donde unidades militares encontraban dificultades para comunicarse con unidades adyacentes con una banda de frecuencias asignada diferente.

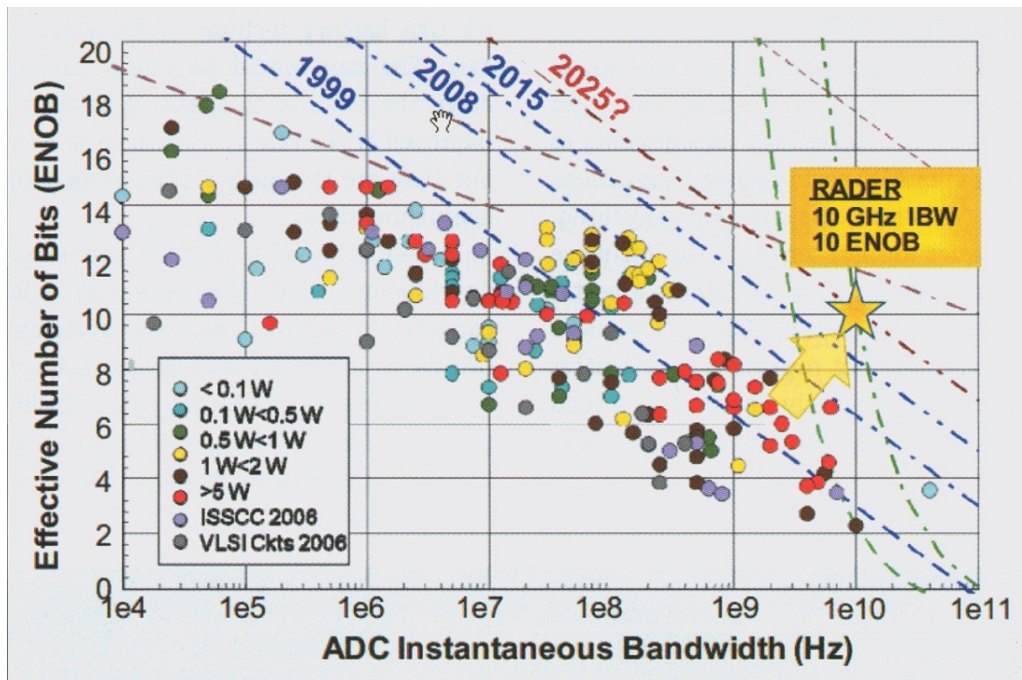
Para paliar estas dificultades, surgieron los sistemas inalámbricos de banda ancha que soportando diferentes tecnologías son capaces de establecer una comunicación de alta capacidad y velocidad en un amplio rango de frecuencias.

El máximo exponente de estos sistemas viene dado por lo que se conoce como SDR o Software Defined Radio (sistemas de radio definidos por software). Estos sistemas se basan en la evolución de los digitalizadores (ADCs y DACs o conversores analógico-digitales y digital-analógico respectivamente), que en los últimos años han logrado un ancho de banda instantáneo y una velocidad de muestreo antes inimaginables.

Estos ADCs y DACs, unidos a un tratamiento de la información mediante sistemas digitales de alta capacidad y velocidad, facilitan la interoperabilidad entre sistemas que operan en bandas de frecuencias distintas y con codificaciones diferentes. En definitiva, como el propio nombre SDR indica, en los sistemas de comunicaciones modernos, la parte de radiofrecuencia queda relegada a un segundo plano cobrando mayor importancia el tratamiento por software de la información conseguida.

En términos de ancho de banda instantáneo, el estado del arte actual en ADCs está dado por el TADC-1000 de Tektronix Component Solutions, ofreciendo una velocidad de muestreo de 12,5 Gmuestras/segundo, BW instantáneo de DC a 6GHz y 8 bits de resolución según hoja de características (7 bits efectivos o ENOB "Effective Number Of Bits")

En la Figura 17 se puede observar el estado del arte de los ADCs y su evolución prevista hasta el 2025.



ADC ENOB Versus Instantaneous Bandwidth (2008). Credit: Dr. Robert H. Walden, The Aerospace Corporation.

Figura 17: Comparativa ENOB vs Ancho de Banda Instantánea

(Fuente: "ADCs and DACs in EW: Far More Than Bit Players" JED – Journal of Electronic Defense, Febrero 2012")

4.3 Enlaces de datos tácticos

Los enlaces de datos (o data link) se pueden definir como enlaces de comunicaciones aprobados y estandarizados, que son adecuados para transmitir información digital. Los TDL (enlaces de datos tácticos) comunican dos o más sistemas C3 para el intercambio de información táctica. En la OTAN, uno de los sistemas más utilizados es el Link16, por ser uno de los servicios digitales del JTIDS/MIDS (Joint Tactical Information Distribution System / Multifunctional Information Distribution System), pertenecientes al acuerdo de estandarización STANAG 5516 / MIL-STD-6016.

Gracias a Link 16, tanto los aviones militares como los barcos y fuerzas terrestres, pueden intercambiar su imagen táctica casi en tiempo real. La información típicamente se envía en una de estas tres velocidades: 31.6, 57.6 o 115.2 kbps, aunque las radios y las propias formas de onda pueden soportar caudales de subida de hasta 238 kbps. También soporta el intercambio de mensajes de texto, datos de imágenes y proporciona dos canales de voz digital (2,4 kbps y/o 16 kbps en cualquier combinación).

Se trata de un sistema seguro, basado en TDMA, resistente a perturbaciones;

enlace de datos digital de alta velocidad en la banda de 960 – 1215 MHz. Este rango de frecuencias limita el intercambio de información a los usuarios que estén en el rango LOS, aunque las tecnologías emergentes proporcionan la transformación entre Link 16 y otros protocolos.

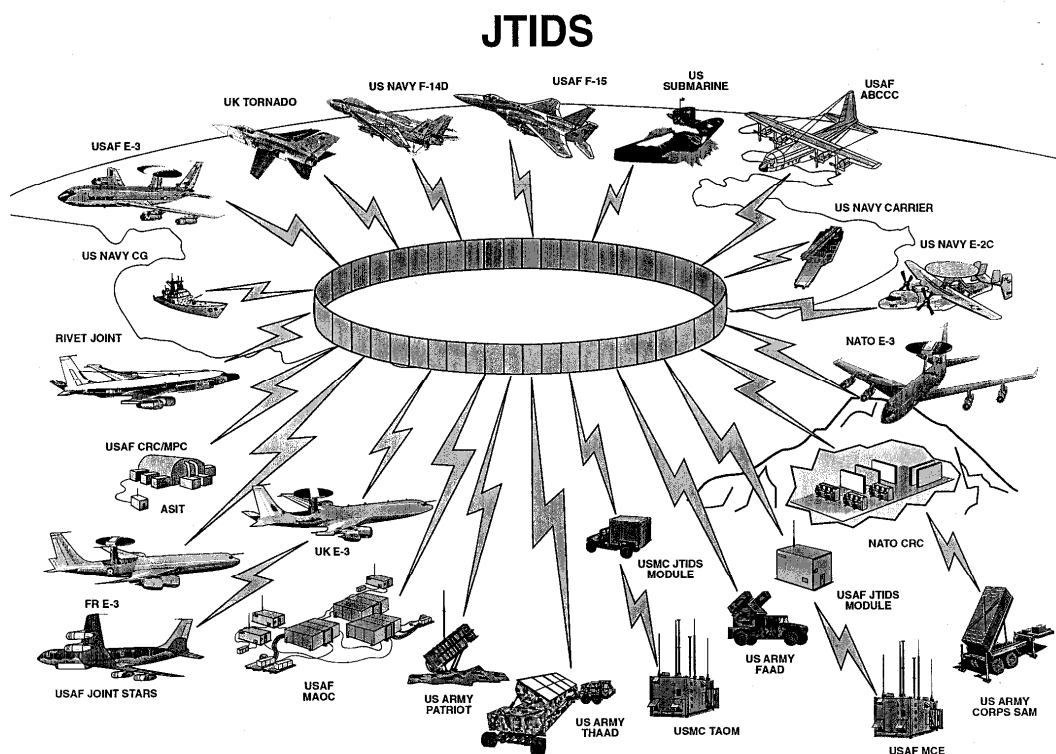


Figura 18: JTIDS. Intercambio de información en Link 16

(Fuente: <http://www.fas.org/man/dod-101/sys/land/image69.gif>)

4.4 Sistemas de comunicaciones por satélite

La utilización de satélites para establecer comunicaciones militares tiene como principal ventaja el acceso a grandes áreas de la superficie terrestre con una infraestructura mínima. Por otro lado es difícil acceder a las órbitas en que se sitúan los satélites por lo que son sistemas muy seguros: muy pocos países disponen de capacidad para destruirlos y se requieren equipos relativamente sofisticados para interferirlos.

También tienen limitaciones muy significativas. Son sistemas muy complejos, de elevado coste y que requieren unas tecnologías muy sofisticadas. Por otro lado, la lejanía entre el satélite y los usuarios, implica la transmisión de elevadas potencias, el empleo de antenas de grandes tamaños y equipos receptores de sensibilidades muy elevadas. A pesar de ello, son los sistemas de comunicaciones más fiables en



escenarios de conflicto, siendo especialmente útiles para:

- El despliegue rápido de redes y servicios en zonas que carecen de infraestructuras.
- Sustituir a las infraestructuras terrestres destruidas, perturbadas o saturadas como consecuencia de los acontecimientos ocurridos en una situación de crisis.
- La interconexión de unidades militares desplegadas en grandes áreas. Es el caso de las actuales misiones de paz donde deben operar coordinadamente ejércitos de diferentes naciones cubriendo en algunos casos un país completamente.
- El establecimiento de la interoperabilidad entre redes y servicios ya desplegados.
- La implantación de sistemas de radiodifusión en zonas extensas

Los sistemas de comunicaciones por satélite se emplean tanto para aplicaciones estratégicas como tácticas, siendo en el segmento de usuarios donde radican las principales diferencias entre ellas. La evolución de estos sistemas irá orientada a superar las limitaciones de los actuales sistemas, entre otras, las restricciones en el ancho de banda utilizable y flexibilidad de utilización. Concretamente, cabe esperar en los próximos años importantes avances en los siguientes campos:

Disponibilidad de mayores anchos de banda de los sistemas, configurables bajo demanda en función de las necesidades específicas de cada usuario en cada momento.

- Reconfigurabilidad de los equipos, incluyendo el uso de antenas adaptativas multi-haz en el segmento espacial para que también las funcionalidades y las coberturas sean configurables.
- Evolución de los terminales hacia una gran variedad de tipos de estaciones en el segmento terreno (fijas, móviles, portátiles), de menor tamaño y coste, y dotándoles de una inteligencia equivalente a la disponible en los terminales de los sistemas terrestres más avanzados.
- Desarrollo de sistemas de protección contra interferencias provocadas o accidentales, dotándoles de la capacidad de trabajar en entornos de guerra electrónica y ciberataques.
- Desarrollo de constelaciones de satélites con enlaces entre ellos para incrementar las posibilidades de enrutamiento y la protección frente a



indisponibilidades de los sistemas de tierra.

- La utilización de nuevas bandas de frecuencias y la utilización de terminales multifrecuencia que puedan trabajar con diferentes bandas del sistema o con sistemas diferentes pero complementarios.
- La gestión eficiente del espectro radioeléctrico ante la multiplicidad de sistemas y sus posibles necesidades urgentes de despliegue.
- Desarrollo de sistemas de integración con redes de satélite civiles, con los consiguientes ahorros de coste y mejoras de disponibilidad. Las diversas alternativas de uso (utilización bajo demanda, capacidades pre-asignadas, etc.) deberán adaptarse a las rigurosas exigencias que imponen las aplicaciones militares a las redes civiles. Dada la importancia en el campo civil de las comunicaciones por satélite esta colaboración civil-militar irá mucho más lejos y cabe afirmar que las soluciones duales se implantarán con carácter general en el desarrollo de las infraestructuras y servicios.

Desde el punto de vista operativo el objetivo final es que estos sistemas consigan una integración con los teléfonos inteligentes y otras tecnologías de comunicación comercial de modo que la cobertura sea prácticamente universal y ubicua. Programas ya en desarrollo como el "Software Reprogrammable Payload (SRP)" pretenden transformar un receptor de radio diseñado para aplicaciones espaciales y en una auténtica plataforma de comunicación diseñada para múltiples funciones, incluidas las comunicaciones, sensores de RF y guerra electrónica en un solo paquete que está implementado sobre una plataforma de software de radio. Su primera aplicación permitirá a los infantes de marina situados en la superficie terrestre conectar, a través de vehículos no tripulados y de estos con satélites, con otros aviones de combate, independientemente de la radio, la red o forma de onda que se utiliza. En definitiva un desarrollo compatible con JTRS y con una arquitectura similar que está definiendo el futuro de estos sistemas.

4.5 Otros sistemas

Existen otros sistemas realizados con los mismos soportes tecnológicos no considerados en los apartados anteriores pero que permiten funcionalidades de gran importancia en el combate moderno. Entre ellos destacan los sistemas de Guerra (EW), Inteligencia Electrónica (ELINT) e Inteligencia de Comunicaciones (COMINT); los sistemas de encriptación de las comunicaciones, los sistemas de identificación y los sistemas de generación y difusión de información audiovisual (MEDIANET).



5 TECNOLOGÍAS CLAVE

En los siguientes párrafos se describirán brevemente algunos de los ámbitos tecnológicos más relevantes que soportan los futuros sistemas de comunicaciones. En cada uno de ellos se detallarán sus características principales, los problemas/retos a los que se enfrentan y las principales soluciones/tendencias que apuntan los tecnólogos y los mercados.

5.1 Terminales inteligentes y de reducido tamaño, peso, consumo y coste (Smart devices, tablets, ...)

Los terminales móviles inteligentes como teléfonos móviles con conexión a datos (o Smartphones), tabletas, etc., están progresivamente pasando de ser un bien de consumo a gadgets utilizados para aumentar la productividad en el ámbito empresarial. En Defensa esto no es una excepción.

– Características principales:

La capacidad de cálculo y de procesamiento de estos equipos ha aumentado exponencialmente en los últimos años, de forma que hoy en día cada vez más llevamos encima a diario un procesador potente que puede ser utilizado para una infinidad de tareas diferentes.

En EEUU ha habido diversas noticias de implantación de aplicaciones, principalmente sobre Android aunque también sobre otros Sistemas Operativos móviles, para militares en campaña.

– Problemas/retos detectados:

Uno de los aspectos fundamentales para que este tipo de dispositivos tenga expansión en el mercado militar pasa por la generalización de su uso en los Puestos de Mando, para ello se requiere la capacidad de cifrar las comunicaciones en este entorno, donde la tecnología apunta a soluciones de tipo WiFi segura. Este es un aspecto fundamental para el desarrollo de aplicaciones de trabajo colaborativo en los puestos de mando operacionales y en los tácticos de grandes unidades.

Así mismo el uso de teléfonos inteligentes, al ser un elemento altamente vulnerable y susceptible de extravío, robo e interceptación requiere para su uso en entornos militares que se les dote de dos capacidades: una de “robustecimiento” físico del propio dispositivo y otra de seguridad en las comunicaciones y aplicaciones relacionadas con su uso militar.



– **Soluciones/tendencias:**

Tanto en nuestro país como en el extranjero se están utilizando aplicaciones creadas para cifrar comunicaciones entre diferentes terminales de forma que por software, sin necesidad de emplear un espectro distinto al que ofrecen las comunicaciones móviles GSM/UMTS, se puede encriptar la comunicación con total garantía. Estas aplicaciones, además permiten hacer un uso dual del mismo terminal, trabajando de manera segura o en uso normal dependiendo de la aplicación que se esté utilizando.

5.2 Radio cognitiva y SDR, interoperabilidad semántica en formas de onda...

La radio cognitiva es un paradigma de la comunicación vía radio pues son equipos que cambian sus parámetros particulares de transmisión o de recepción para llevar a cabo la comunicación de forma eficiente sin interferir a los usuarios autorizados. La alteración de los parámetros de la radio está basada en la monitorización activa de varios factores en el entorno externo e interno de la radio, tales como el espectro radioeléctrico, el comportamiento del usuario o el estado de la red, para lo que debe de analizar y clasificar las emisiones, predecir los patrones implicados y elegir el mejor método de transmitir su información.

– **Características principales:**

La Radio Definida por Software (Software Defined Radio, SDR) es un sistema de radiocomunicaciones donde los componentes de RF se reducen al mínimo porque las tradicionales funciones de filtrado, conversión de frecuencia, amplificación, generación de señal, detección etc., se realizan mediante algoritmos numéricos, una vez que la señal ha sido digitalizada en un conversor analógico/digital (A/D) de alta velocidad.

Idealmente, la parte de RF estará formada sólo por una antena, un filtro y un amplificador que cubren la banda de trabajo de la radio, típicamente varias octavas, cuya salida ataca al A/D.

La SDR tiene ventajas asociadas a los costes de los equipos (se comparte el hardware y se implementan los diferentes estándares mediante cambios de software), pero sobre todo lo que aporta es una flexibilidad casi total al poder seleccionar numerosas formas de onda y protocolos previamente almacenados para operar. Además, el concepto SDR se asocia a la posibilidad de enviar y transmitir en grandes anchos de banda (existen desarrollos que cubren prácticamente todas las bandas de las comunicaciones tácticas: de algunos MHz a casi 3 GHz), a la búsqueda de la interoperabilidad con sistemas heredados y a la utilización de



elementos COTS. A largo plazo, se confía en que será la tecnología dominante en radiocomunicaciones, pues es la que permite implementar el concepto de radio cognitiva.

– **Problemas/retos detectados:**

En estos momentos, las limitaciones en la capacidad de digitalización de los actuales A/D y en las velocidades de los procesadores digitales de señal obligan en muchos casos a complicar la RF. Sin embargo la tendencia tecnológica es a reducir los subsistemas de RF al mínimo, en la medida que se consigan aumentos en las velocidades de digitalización y proceso.

– **Soluciones/tendencias:**

El gran número de emisiones simultáneas presentes en los futuros escenarios, cada vez transmitiendo más información y por tanto consumiendo más banda de frecuencia, plantea crecientes problemas en la gestión del espectro electromagnético al objeto de evitar las interferencias accidentales o provocadas sobre comunicaciones tácticas en muchos casos de vital importancia.

Las radios cognitivas serán imprescindibles en algunos sistemas de comunicaciones, tanto civiles como militares, eliminando la necesidad de una gestión planificada exhaustiva previa del espectro. Además son mucho más resistentes a intrusiones o perturbaciones de ataques electrónicos y, por su propia concepción, interoperables. Nótese que todas estas características son muy necesarias en misiones expedicionarias como las que tratamos en estas páginas.

Finalmente, conviene resaltar que los avances tecnológicos previsibles en el los próximos años -con el imparable desarrollo de procesadores más potentes y algoritmos más sofisticados- son el principal aval de estas nuevas radios. Por el contrario, razones de orden político –asociadas a los derechos sobre el espectro electromagnético de diferentes organismos y operadores- constituyen el principal obstáculo a su implantación. En efecto, los reguladores asignan bloques de espectro compartidos o en exclusiva a usuarios específicos, lo que puede evitar que radios cognitivas conmuten a la frecuencia mejor posible, incluso si no se está utilizando en ese momento, simplemente debido a que el canal se encuentra dentro de una banda atribuida a otro usuario. Obviamente en el campo militar esta limitación puede ser superada con mayor facilidad.



5.3 Gestión dinámica del espectro y nuevas formas de onda (WiMax securizado, LTE securizado, ...)

La gestión dinámica del espectro (DSM por sus siglas en inglés) o gestión dinámica de acceso (DSA) consiste en una serie de técnicas espectrales que se utilizan para mejorar y optimizar la comunicación de un sistema de comunicaciones.

El concepto de DSM ha sido posible gracias a la disponibilidad de SDR, debido al desarrollo de procesadores suficientemente rápido tanto en servidores como en terminales. El DSM se utiliza mayormente para sistemas DSL, aunque también se están realizando investigaciones en el ámbito de la radio cognitiva.

– Características principales:

Los principios comunes a los métodos DSM incluyen:

- Adaptación del enlace de comunicaciones.
- Gestión del ancho de banda.
- MIMO multiusuario.
- Pre-cancelación de la interferencia estimada.
- Combinación de canales sin usar (o sin reservar) para un único usuario o adhesiones (redundancias).

Las técnicas más comunes son:

- Métodos de identificación del canal
- Balanceado espectral
- Métodos de transmisión vectorial
- Detección de multiusuario

– Problemas/retos detectados:

Hay que revisar el nivel de seguridad en entornos de LTE y WiMax para encontrar los requisitos operativos militares que se consideren necesarios.

– Soluciones/tendencias:

Long-Term Evolution (LTE) es la próxima generación más allá de las redes 3G. LTE utiliza OFDM (orthogonal frequency-division multiplexing) en la tecnología de acceso de radio, junto con tecnologías avanzadas de antena. Además de LTE, 3G ha



especificado un modelo plano de acceso a la red, basado en una arquitectura de red IP. Es la evolución natural de las topologías de red 3GPP GSM, WCDMA, WiMAX y 3GPP2 CDMA.

LTE debe proporcionar al menos el mismo nivel de seguridad que 3G, y minimizar el efecto sobre los cambios en la arquitectura IP descrita anteriormente. El servicio de autenticación es uno de los servicios más esenciales en redes LTE, lo que tiene efectos significativos sobre la seguridad en Internet. Por otra parte, algunos trabajos futuros para la interoperabilidad entre redes LTE y su antecesor WiMAX deben ser implementados, por cuestiones de amortización de equipamiento ya existente.

La seguridad en redes inalámbricas ha sido tradicionalmente considerada como un tema a tratar en las capas superiores de la red. Mientras que la demanda para aplicaciones tales como mensajería de texto corto (SMS) y acceso WAP, la mensajería multimedia (MMS) y las descargas de contenido tiene la necesidad de mayor ancho de banda, debido a que ya se introducen las aplicaciones de vídeo compartido y televisión sobre IP (IPTV), cuya demanda está creciendo rápidamente. Con este crecimiento, las amenazas de seguridad cada vez mayores también necesitan que las nuevas redes cuenten con alta seguridad de cara a crear la confianza en el usuario, a través de las correspondientes políticas de privacidad.

A todo ello debe añadirse que se debe encontrar la manera de asegurar las comunicaciones por enlace de datos (en las capas más inferiores de la red) mediante la encriptación de las mismas en el nivel de enlace. Un nuevo tipo de dispositivo criptográfico (punto a multipunto) debe ser desarrollado e implementado para estas aplicaciones.

5.4 Redes inalámbricas ad-hoc (MESH, MANET...)

Las Redes inalámbricas Ad Hoc (o MANETs, del inglés Mobile Adhoc NETWORKs) son un tipo de redes inalámbricas llevadas al extremo: no es necesaria ninguna infraestructura previa para comunicarse a través de la red. Los equipos o nodos que forman parte de ella se organizan por sí mismos para ayudarse los unos a los otros en el proceso de transportar paquetes de datos entre un origen y un destino.

– Características principales:

- Movilidad: todos los nodos de la red pueden ser móviles
- Flexibilidad:
 - o No es necesaria infraestructura previa



o Red auto-gestionada

El objetivo de estas nuevas redes es disponer en el campo de batalla de nodos de comunicaciones móviles, de despliegue rápido y flexible, auto-adaptables a la topología cambiante de los diferentes y que permitan la comunicación multisalto entre ellos, es decir, que no sea necesario disponer de un enlace radio directo entre dos nodos para poder establecer un servicio de comunicación entre ellos.

El corazón de un sistema ad-hoc es el conjunto de protocolos implementados en él que permiten que cada nodo del sistema, una vez se encuentra en funcionamiento, se integre de forma automática en la red asignada, lo que implica la implementación de, al menos, las funcionalidades de identificación, reconocimiento de topología y cálculo de rutas. En el caso de las redes móviles, es necesaria también otra funcionalidad relacionada con la gestión del enlace ad-hoc de nodos en movimiento.

Algunos ejemplos de enrutamiento dinámico:

- Ad-hoc On-Demand Distance Vector (AODV) definido en la RFC 3561¹
- Optimized Link State Routing Protocol (OLSR) definido en la RFC 3626²

Algunas de las posibilidades que ofrecen estos nuevos protocolos de enrutamiento son, entre otros, la optimización dinámica del uso de ancho de banda, la disponibilidad de servicios distribuidos independientemente de su localización física, la gestión automática facilitando el acceso tanto a nivel local como remoto por los operadores a través de un terminal de gestión, la movilidad total de usuarios cuyos terminales se conectan automáticamente utilizando tantos saltos y pasarelas reconfigurables como sea necesario y la reconfiguración automática de la red sin pérdidas de datos asegurando la capacidad de los enlaces.

– Problemas / Retos Detectados:

Los retos a los que se enfrentan este tipo de redes pasan desde lo primarios, como son: aumentar movilidad, rango y ancho de banda, a los propios de entorno de zona de operaciones como son: i) conectividad del terminal con los equipos existentes, ii) posibilidad de usar las tecnologías existentes, manteniendo las comunicaciones en ZO, y soportados por el ruteo mallado móvil de la red MANET en caso de falta de infraestructura y iii) eficiente y robusta securización soportada por

¹ Perkins C., Belding-Royer E., Das S., "Ad hoc On-Demand Distance Vector (AODV) Routing." Network Working Group Request for Comments: 3561. <http://www.ietf.org/rfc/rfc3561.txt>.

² Clausen T., Jacquet P., "Optimized Link State Routing Protocol (OLSR)." Network Working Group Request for Comments: 3626. <http://www.ietf.org/rfc/rfc3626.txt>.



los protocolos de enrutamiento.

Y los problemas que debe minimizar o solventar son:

- Limitaciones geográficas y del terreno
- Limitaciones tecnológicas, como memoria de los terminales, potencia y autonomía necesarios.
- Ataques: posibles rupturas de los códigos de encriptación, ataques DoS (Denial of Service)

– **Soluciones/tendencias:**

Debido a la escasa infraestructura de las redes en entornos militares, la cuarta generación móvil o LTE (long term evolution) es la solución para alcanzar transmisiones de alta calidad y conectividad constante en las MANETs. Proporciona un único interfaz para todos los tipos de redes inalámbricas permitiendo a los nodos participantes a acceder a la red a través de red móvil, inalámbrica, y protocolos como IEEE 802.20 y WiMax.

Sin embargo, su implementación en entorno militar es significativamente más complicada debido a los requisitos únicos de especificación.

En cuanto a protocolos de enrutamiento, en los próximos años tendrán especial relevancia el desarrollo de los mismos para redes tácticas de bajo ancho de banda, los orientados a redes de sensores desatendidos y los utilizados para gestionar los enlaces de datos en operaciones de vehículos no tripulados, aunque cabe esperar que esta tecnología se extienda a otras muchas aplicaciones. Hasta el momento se han desarrollado diferentes protocolos MANET, principalmente asociados a radios de banda ancha como SDR y la última generación de radios UHF de soldado.

5.5 Sistemas bastionados de Identificación, Autenticación...

Los sistemas bastionados son sistemas identificados por el firewall administrador de una red como un punto fuerte crítico en la seguridad de la red. Generalmente a los sistemas bastionados se les aplica una seguridad extra; pueden llevarse a cabo auditorías regulares y pueden tener software modificado a propósito para el cumplimiento de su tarea.

– **Características principales:**

Consisten principalmente en un ordenador que diseñado específicamente y



configurado para resistir ataques. Éste, generalmente, hospeda una única aplicación, por ejemplo un servidor proxy y el resto de servicios se eliminan o limitan al máximo para reducir las amenazas a este ordenador.

Esta forma de configuración se debe principalmente a la localización y propósito del sistema, que se encuentra o bien fuera del firewall o bien en la DMZ habitualmente identificando o autenticando información procedente de redes no fiables.

Localización

Hay dos configuraciones comunes de red que incluyen sistemas bastionados y su colocación. La primera requiere dos firewalls, con sistemas bastionados colocados entre el firewall del “mundo exterior” y un firewall interior situado en una DMZ. Habitualmente redes más pequeñas no tienen múltiples firewalls, así que cuando sólo existe uno, los sistemas bastionados se colocan fuera de este.

Ejemplos

Hay distintos ejemplos de sistemas o servicios bastionados:

- Servidor DNS (Domain Name System)
- Servidor de correo electrónico
- Servidor de E-mail
- Servidor FTP
- Honeypot
- Servidor Proxy
- Servidor VPN
- Servidor Web

– Problemas/retos detectados:

Pero bastionar un servidor no solo consiste en aplicar lo anterior, se deben realizar una serie de acciones complementarias que hacen más difícil la penetración del servidor, algunas de ellas son:

- Evitar el acceso via red de los servidores ya que si el atacante penetra en una de las máquinas de la DMZ podrá atacar al resto desde ella.
- Evitar el uso multipropósito de los servidores permitiendo la instalación de software de desarrollo.



- Control de los permisos de los usuarios que tienen acceso al servidor.

– **Soluciones/tendencias:**

Para evitar el tráfico entre servidores de la red DMZ deben emplearse envolturas y reglas de filtrado a nivel local para que en el caso del que el router fuera atacado el servidor no estuviera desprotegido.

Si el servidor es multipropósito con usuarios que acceden al mismo para propósitos ajenos a los que estamos protegiendo, les estamos dando una puerta de atrás de entrada a los datos que hemos bastionado en el servidor, es decir, tenemos que controlar las herramientas, los permisos y los flujos de datos.

Cada servicio de la máquina debe ejecutarse con un usuario/grupo propio y unico para cada servicio, ya que si se consigue explotar una vulnerabilidad desde uno de ellos, como por ejemplo, www-data o ftp, una vulnerabilidad de dicho servicio solo le afectaría a él y no comprometería al resto de los servicios de la máquina, que estarían ligados a otros usuarios.

Finalmente no conviene olvidar que además de bastionar un servidor debemos aplicar las normas básicas de protección de cualquier sistema de información, realizar copias de seguridad, configurar la red para la detección de intrusos y para mantener la integridad de los datos (aide, tripwire, etc.) y disponer de un sistema de logs local y central.

5.6 Antenas inteligentes, sistemas multisensor...

Los sistemas multisensor o en definitiva sistemas de múltiples entradas conocidas como array de antenas adaptativas o antenas inteligentes, son arrays de antenas o sensores que utilizan algoritmos inteligentes de procesamiento para identificar los diferentes parámetros de la señal recibida como la DOA (Dirección de Llegada de la señal – Direction Of Arrival) así como para mejorar la relación señal a ruido de la señal recibida, aumentando de este modo sensiblemente la calidad del enlace, mediante la conformación del haz para situar máximos en la dirección de la emisión deseada y nulos en las interferentes.

– **Características principales:**

Dos de los principales tipos de antenas inteligentes incluyen antenas de lóbulo conmutado y antenas de array adaptativo. Las primeras tienen diferentes lóbulos fijos disponibles. En un determinado instante, basándose en los requisitos del sistema, se toma la decisión de a qué lóbulo acceder. Por el contrario, los arrays



adaptativos permiten a la antena sincronizar el lóbulo a cualquier dirección de interés mientras se anulan las señales interferentes. La dirección del lóbulo se puede encontrar usando los métodos de estimación tipo DOA.

– **Problemas/retos:**

Este tipo de antenas son aplicables a casi todos los protocolos y estándares inalámbricos y en general a todos los sistemas que tengan que trabajar en un entorno radioeléctrico complejo (por ejemplo por existencia de multirayectos o interferencias. Es una tecnología que permite aumentar la eficacia del uso del espectro, mediante el control inteligente de la iluminación. Sus principales retos son la necesidad de disminuir los costes, tamaños y pesos de los numerosos subsistemas de radiofrecuencia requeridos, así como de los complejos procesadores de señal, sobre todo en los sistemas portátiles y terminales.

– **Soluciones/tendencias:**

Multiple-Input Multiple-output (MIMO) es una de las tecnologías de este tipo de antenas que se usan en WIMAX y que aprovecha el fenómeno de la multipropagación y el empleo de la diversidad del espacio que permite conseguir una mayor velocidad y un mejor alcance que el de las antenas convencionales.

La capacidad de un sistema MIMO, cuando las señales recibidas no están correlacionadas entre si, es proporcional al número de antenas empleadas con el consiguiente incremento del coste de fabricación. El diseño de las antenas busca reducir la correlación entre las señales recibidas utilizando diferentes modos de diversidad, la de espacio, la de ganancia y la de polarización.

La incorporación de procesadores en las antenas inteligentes permiten variar dinámicamente el patrón de las mismas permitiendo un uso más eficiente y una reducción de costes por su adaptabilidad a diferentes entornos operativos.

5.7 Soporte inteligente a las TIC: Minería de Datos (Data Mining), Big Data Technologies...

En el ámbito TIC nos referimos a Big Data cuando el conjunto de datos adquirido por un sistema de comunicaciones o transmitido por este, es tan grande y complejo que llega a ser difícil de procesar usando herramientas tradicionales de bases de datos o aplicaciones de procesado.

– **Características principales:**

Dado el desarrollo de los sistemas TIC en los últimos años, el aumento en los anchos de banda de los sistemas transmisión, y la digitalización a gran velocidad



(sistemas SDR), la evolución ha obligado a incrementar el rendimiento del procesado de los datos adquiridos y transmitidos surgiendo las tecnologías Big Data.

– **Problemas/retos:**

Los principales retos incluyen la captura de los datos, selección, almacenamiento, búsqueda, compartición, análisis y visualización.

– **Soluciones/tendencias:**

La tendencia hacia mayores conjuntos de datos se debe a la información adicional derivable del análisis de un único conjunto grande de datos relacionados, comparado con conjuntos más pequeños, separados, con la misma cantidad de datos. En los conjuntos mayores se pueden encontrar mayores correlaciones.

Así pues dentro de esta evolución, han surgido recientemente campos novedosos como la minería de datos (o Data Mining) que consisten en descubrir patrones comunes en conjuntos de datos grandes. Este campo se encuentra a mitad de camino entre las TIC y la estadística, y utiliza métodos que combinan inteligencia artificial, aprendizaje de máquinas, estadística y sistemas de bases de datos. Además del análisis de datos sin procesar, la minería de datos engloba también aspectos de gestión de datos, preprocesado, postprocesado, visualización, actualización on-line y otras consideraciones.



6 LAS FUERZAS ARMADAS ESPAÑOLAS ANTE EL RETO DE LAS FUTURAS COMUNICACIONES MILITARES

La unidad de esfuerzos de todos los componentes de una operación internacional de mantenimiento de la paz, así como la cooperación entre todos los órganos competentes en la materia, se debe establecer desde el principio de una misión y deben estar previstos en el proceso de planificación. La sede de nivel estratégico (ó Cuartel General) debe desarrollar concepto de las operaciones (CONOPS) y coordinar la generación inicial de Fuerzas. Al mismo tiempo, un plan de misión coordinado debe estar preparado a nivel operativo y debe ser coordinado bajo un Jefe de Misión, reuniendo todos los componentes de la misión, incluyendo la asignación de tareas y prioridades y aspectos logísticos. Debe darse un tiempo para la adecuada formación de la sede para la misión antes del despliegue de la misión.

La plena integración de todos los implicados en una operación con aspectos multifuncionales, es a menudo difícil de lograr debido a los muchos y muy diversos integrantes en cualquier teatro de operaciones internacional, siendo necesario un Jefe de Misión en sintonía con ambas culturas (civiles y militares) de gran ayuda para la coordinación, cooperación e integración de todas las Fuerzas implicadas. A juicio de algunos países, un centro de operaciones cívico-militares es la mejor manera de asegurar la coordinación y la integración, ya que la cooperación interdisciplinar y una estructura jerárquica no son mutuamente excluyentes. Debe haber una cooperación muy estrecha entre los componentes civiles (políticos) y militares de una operación de mantenimiento de la paz, de cara al entendimiento para que no surjan situaciones indeseables (los militares no se deben utilizar en tareas policiales para las que no han sido entrenados, por ejemplo).

Conforme a todo lo anteriormente expuesto, se necesitan medios idóneos para labores de Mando y Control de toda la estructura dispuesta, que deben estar claramente definidos y acordados antes de la implementación de la misión de paz. Es necesario establecer las responsabilidades a todos los niveles de la estructura de mando, para aclarar los procedimientos y relaciones de trabajo dentro de la misión, así como establecer los procedimientos de comunicaciones y apoyo logístico que sean compatibles con las necesidades de la misión. Los elementos de Mando y Control deben incluir los medios para intercomunicarse los diversos equipos que componen la misión y establecer su coordinación, así como la selección de los medios de interconexión con la sede estratégica con la que se demandará la coordinación.

Los medios CIS de apoyo (Communications and Information Systems) dentro de la zona de operaciones y de cara a la conexión con la sede estratégica, hasta el más alto nivel de mando, deben ser cuidadosamente planeados antes del despliegue de



las fuerzas. El objetivo debe ser lograr la interoperabilidad de los CIS utilizados por la organización supranacional que lidera la operación, y los utilizados por las Naciones que aportan contingentes de tropas (TCNs - Troops Contributing Nations). Existen requisitos por tanto para la normalización, relativos al nivel de interoperabilidad técnica, y para el nivel de uniformidad de la información en torno a los procedimientos utilizados.

La coordinación con los elementos nacionales de terceros países ajenos a la organización supranacional que lidera la misión, las pruebas de interoperabilidad de los CIS utilizados, y la capacitación de los procedimientos operativos C4ISR antes del despliegue, ayudarán al correcto flujo de información durante las operaciones. Muchas tecnologías estarán implicadas en el correcto desarrollo de todo lo expuesto, las cuales han sido detalladas anteriormente en el capítulo 5.

Para acabar, como lecciones específicas aprendidas, algunos países consideran que las capacidades necesarias CIS en los entornos operacionales descritos se incluyen o resumen en los siguientes puntos:

- o En el teatro de operaciones, los medios CIS deben gestionarse de forma centralizada por la Célula de Apoyo CIS con la que debe contar la sede estratégica, si bien la operación de los mismos debe darse de forma descentralizada;
- o Las Fuerzas desplegadas deben utilizar las infraestructuras de comunicaciones locales comerciales del país de acogida para la misión. Sin embargo, tanto los elementos civiles como los militares de las Fuerzas desplegadas no deben utilizar dichas infraestructuras como medio principal de comunicación;
- o Las Fuerzas desplegadas deben controlar sus propios medios CIS;
- o Debe contarse con el máximo aprovechamiento del espectro radioeléctrico como recurso finito;
- o Las comunicaciones tácticas deben basarse en radios VHF tipo "Red de Combate", como medios primarios en la zona geográfica a cubrir, a no ser que el terreno cubierto demande el uso de otros medios, como SATCOM táctico (TACSAT) por ejemplo;
- o Redes de Radios de combate en la banda HF pueden ser utilizadas como sistemas de respaldo. Los enlaces con los medios CIS proporcionados por los países de acogida pueden también basarse en SATCOM comercial (Inmarsat, Thurayah, Iridium...);
- o Medios relativos a Conciencia Situacional se estiman necesarios. Para ello,



los sistemas globales de navegación por satélite (GNSS) son herramientas de apoyo muy útiles para establecer comunicaciones con elementos itinerantes;

- o El Cifrado y las capacidades de Ciberseguridad son un punto clave para el desarrollo de la misión;
- o La computación en la nube (Cloud Computing) puede ser clave para garantizar los datos de misión. Para ello, la coalición internacional debe aportar, gestionar y controlar su propia nube (Cloud in-the-can).



7 EL SECTOR DE LA DEFENSA Y SEGURIDAD ANTE EL RETO DE LAS FUTURAS COMUNICACIONES MILITARES

La conclusión que se extrae de los apartados anteriores no es otra que los despliegues de nuestras Fuerzas Armadas en el exterior estarán soportados por unas tecnologías muy complejas cuya disponibilidad y dominio será esencial para el éxito de las misiones, junto a la correcta formación de los operadores y mandos. Todo ello enmarcado en nuevas doctrinas y estructuras organizativas adaptadas a las características de los conflictos y de los medios disponibles para su resolución.

La cuestión clave es como conseguir que nuestras Fuerzas Armadas dispongan de estas tecnologías y sistemas asegurando que se obtendrá el máximo valor añadido para nuestro país. Lo importante es optimizar los procedimientos y procesos para pasar de los conocimientos generados en nuestros centros de investigación – públicos y privados- y nuestras universidades a unos productos, en la medida de lo posible fabricados una la industria nacional, que satisfagan las necesidades a unos costes asumibles.

Por otro lado, hay pocas dudas sobre la globalización generalizada de los mercados y la consecuente internacionalización de las actividades empresariales. El desarrollo de proyectos conjuntos con nuestros aliados o las políticas del tipo “*pulling and sharing*” convivirán junto con algunas iniciativas propias cuya adecuada selección definirá el éxito de las mismas.

7.1 Una oportunidad para la Industria de Defensa en España

La preocupación por la componente tecnológica de nuestros Ejércitos la podemos situar en la creación del Ministerio de Defensa en el año 1977, de hecho la Dirección General de Armamento y Material ya aparece en la primera organización del ministerio definida en el Real Decreto 2723/77. Desde entonces esta preocupación se ha mantenido, en paralelo con los procesos de profesionalización y modernización de las Fuerzas Armadas, y en las numerosas reorganizaciones que éstas han sufrido siempre se ha aludido a este aspecto. Sin embargo, en términos presupuestarios, este esfuerzo ha estado sometido a los avatares de la política y la situación económica del momento.

Lo que es innegable es que en los últimos 30 años esta preocupación se ha manifestado en una política inversora y de apoyo a la I+D que ha permitido consolidar un tejido industrial en el sector de Defensa que aporta tecnologías y vende sofisticados sistemas duales en el mercado exterior. Una industria que en estos momentos está padeciendo las consecuencias de la crisis económica con gran



intensidad, entre otras cosas, como consecuencia de la disminución drástica de inversiones del Ministerio de Defensa. Una industria que está sometida a un proceso de concentración y reconversión cuyas consecuencias son inciertas.

En el último párrafo de la Directiva de Defensa Nacional publicada el julio del 2012, se afirma: “... la Defensa de España exige el impulso de la industria nacional del sector, suministrador idóneo de las necesidades de nuestras Fuerzas Armadas...”. Para indicar a continuación que “En los tiempos actuales, la permanencia y desarrollo de la misma hace precisa la asistencia a esta en su presencia internacional, especialmente en la penetración en mercados que por su especificidad observan garantías mayores con el respaldo de Estado a Estado.”.

En definitiva se ofrece un apoyo -seguramente que muy necesario y eficaz- que requiere disponer de sistemas propios previamente desarrollados y probados. Por lo tanto, esta industria seguirá siendo dependiente de las inversiones del Ministerio de Defensa, tanto para financiar unos desarrollos muy costosos, como para demostrar la bondad de sus productos cara a la exportación.

El dominio de las tecnologías objeto de este informe y el desarrollo de los sistemas mencionados en el mismo es algo más que una oportunidad de cara a asegurar que una industria propia suministre a nuestras Fuerzas Armadas. Es posiblemente la condición para que pueda existir una industria propia significativa en el ámbito de las TIC: La dualidad de las tecnologías implicadas y la convergencia entre las aplicaciones civiles y militares hacen difícil imaginar el éxito en este subsector sin una I+D fuertemente apoyada, de modo coordinado, desde los diferentes departamentos de la Administración.

Es en este contexto en el que cabe plantearse cuáles son los principales riesgos y oportunidades que, como país, tenemos para poder desarrollar estas tecnologías y sistemas.

7.2 Riesgos

Existen un conjunto de debilidades estructurales en el subsector de las telecomunicaciones –en buena medida compartidos por los ámbitos civil y militar- que se traducen en un conjunto de riesgos a corto y medio plazo que amenazan no sólo su crecimiento, sino incluso su supervivencia.

- **Dependencia tecnológica.** Una buena parte de sus productos están desarrollados con tecnologías y equipos foráneos, de hecho es muy habitual que las empresas españolas se presenten a los concursos acompañados de socios tecnológicos internacionales. Lo que a corto plazo puede ser muy beneficioso para estas empresas, puede suponer en el próximo futuro la pérdida de ese



sector del mercado por la imposibilidad de competir en precio con los productos que fabrica este socio tecnológico. No podemos olvidar que la tendencia a la concentración de empresas en el ámbito internacional favorece que todas ellas se dediquen a la integración vertical de sistemas y, por tanto, dispongan de productos similares. El riesgo aumenta en la medida que la empresa actúa como mera intermediaria, sin asimilar la tecnología o dotar a los productos de valor añadido, una situación más frecuente de lo que sería deseable.

Las telecomunicaciones militares son especialmente sensibles a esta dependencia por la rápida evolución de su base tecnológica y su creciente servidumbre de un ámbito civil caracterizado por unos mercados en crecimiento exponencial.

- **Globalización y apertura de mercados.** La progresiva internacionalización de nuestras Fuerzas Armadas dificulta la creación de barreras para la protección de la industria nacional y el mantenimiento de conceptos como el de “justo retorno” o los “retornos industriales” por las adquisiciones en otros países. Por otro lado, el paradigma ideológico dominante favorece la apertura de los mercados – una apertura asimétrica que siempre favorece a las industrias más poderosas – y la estandarización de productos. De hecho, en los últimos años se está produciendo un progresivo proceso de liberalización en el sector. La convergencia de este fenómeno con la dependencia tecnológica puede tener consecuencias fáciles de imaginar en un entorno cada día más competitivo.

En este punto conviene resaltar que nuestro país ha perdido la mayor parte de la industria de telecomunicaciones que tenía antes del proceso de liberalización del sector iniciado a finales de los años noventa.

- **Incremento de la complejidad y coste de los sistemas.** Con carácter general, las barreras de entrada a nuevos mercados se ven incrementadas por los elevados tiempos y costes de desarrollo de los equipos. Además, este encarecimiento está produciendo problemas presupuestarios en unas Fuerzas Armadas que pueden percibir el apoyo a una industria nacional como un riesgo en el cumplimiento de sus misiones en la medida que recorta los medios a su disposición. En este punto, es necesario resaltar que, en muchos casos, la idea de que un producto extranjero es más barato que su equivalente nacional es falsa. Obviamente, en principio es más barato adquirir un equipo que desarrollarlo, pero no hay que olvidar que estamos ante productos con elevados ciclos de vida donde los costes de mantenimiento y modernización pueden ser muy superiores a los de adquisición. La experiencia ha demostrado que un producto nacional es mucho más fácil de mantener y adaptar a las futuras necesidades, especialmente si es auténticamente nacional.
- **Abuso del sistemismo.** Para hacer un sistema competitivo se requiere conocer



y dominar las tecnologías que lo soportan. Si una empresa actúa como mera integradora puede llegar a instalar y mantener un sistema – a un coste y con una calidad en muchos casos discutible-, pero los inconvenientes son evidentes:

- Dependencia foránea en el suministro de los repuestos, cuyos costes difícilmente pueden ser controlados por el suministrador nacional del sistema.
- Dificultad, e incluso imposibilidad práctica, de modificaciones significativas durante el ciclo de vida del sistema, especialmente si se pretende una personalización de sus prestaciones.
- Especificación y, sobre todo, evolución de los sistemas con criterios ajenos a nuestras necesidades operativas y apoyando tecnologías e intereses no nacionales.
- Mucho mayor coste en términos de economía nacional y escaso impacto sobre la misma.

Mientras comprar un equipo y cambiarle la etiqueta o interconectarle con otros genere muchos más beneficios que desarrollarlo, existirán defensores acérrimos del sistemismo, pero, ante los cambios en el entorno ya comentados, las preguntas inmediatas son: ¿cuánto tiempo tardarán las empresas matrices en darse cuenta de que esta intermediación es innecesaria o que la pueden reducir al mínimo imprescindible?, ¿cómo puede pedirse a las Fuerzas Armadas que soporten los costes de una intermediación que apenas les aporta nada?.

En el caso de los equipos objeto de este informe, los requerimientos de interoperabilidad forzarán un elevado grado de estandarización que facilitará el desarrollo conjunto de sistemas –la estrategia *“pulling and sharing”* ya mencionada- con nuestros aliados. La correcta gestión de esta colaboración será un elemento esencial para el futuro del subsector.

- **Política de adquisiciones de “riesgo cero”.** El paradigma de todos estos riesgos es el concepto de “riesgo cero” que se atribuye con alguna frecuencia a las compras de equipos extranjeros, especialmente a la adquisición de equipos utilizados por las Fuerzas Armadas de Estados Unidos. Para los gestores, y esto es aplicable a todos los sectores de actividad, es mucho más cómodo y seguro optar por unos productos probados y, por tanto, con más garantías de ser servidos en plazo y funcionando correctamente. Por otro lado, son decisiones muy fáciles de justificar con el argumento de que la obligación de las instituciones es disponer del mejor material para cumplir las misiones que tienen encomendadas.

En muchas ocasiones no son decisiones de riesgo cero sino de alto riesgo ya



que a los efectos negativos producidos por estas decisiones, ya expuestos, hay que añadir dos más. En primer lugar, el material que puede adquirirse “bajo catálogo” y “ya probado” no es de última generación, incluso suelen ser equipos diseñados con tecnologías de hace quince o veinte años debido a sus elevados ciclos de desarrollo y vida, lo cual implica que a medio plazo será desclasificado y aparecerán problemas en su sostenimiento. Por otro lado, en productos con alto contenido en TIC's, ¿quién garantiza que son los mismos que utiliza el país de origen? No debemos olvidar que la mayor parte de las capacidades de los modernos sistemas radica en las aplicaciones software que incorporan, ¿quién garantiza que los programas adquiridos son los últimos que llevan instalados sus sistemas?

Obviamente el ámbito de las telecomunicaciones es imposible la autarquía, no se puede disponer de todas las tecnologías ni desarrollar todos los equipos, por lo que su adquisición e integración es una alternativa necesaria. Pero, incluso en estos casos, es preciso realizar inversiones en infraestructuras y recursos humanos para disponer de medios y conocimientos que permitan optimizar estas adquisiciones, minimizando los efectos negativos mencionados.

7.3 Oportunidades

El subsector de las telecomunicaciones militares, en buena medida por estar ligado a las TIC, también tiene fortalezas y capacidad para afrontar los retos del futuro. Para ello, con la colaboración y el compromiso de todos los agentes, hay que aprovechar las oportunidades que los cambios tecnológicos aportan a su industria:

- **Accesibilidad de las tecnologías.** La horizontalidad, transversalidad y rapidez de evolución de las TIC's facilita su accesibilidad, incluso con algunas ventajas frente a productos ya consolidados. Cada día se encuentran en el mercado nuevos componentes con mejores prestaciones y a menor coste que permite plantearse desarrollos muy competitivos frente a los disponibles en el mercado. Por otro lado, su flexibilidad permite soluciones adaptadas a cada cliente, una ventaja operativa especialmente interesante en aplicaciones militares.

La tendencia a utilizar componentes COST para implementar los equipos de telecomunicaciones basados en dispositivos hardware estandarizados y configurables por software elimina muchas barreras. La oportunidad se ve reforzada por la calidad de la formación que se imparte en nuestro país en este ámbito tecnológico. Nuestros ingenieros y técnicos han demostrado que, dotados de los medios adecuados, son capaces de realizar con éxito los sistemas más avanzados.



- **Especialización en áreas concretas de actividad.** La correcta selección de los nichos tecnológicos y aplicaciones donde las capacidades de nuestra industria aporten mayor valor añadido será clave en su éxito. Por otro lado, en la medida de lo posible deberán seleccionarse áreas tecnológicamente duales, que faciliten la transferencia de los esfuerzos y resultados al campo civil, y viceversa. Países de dimensiones similares, e incluso menores al nuestro, ya han recorrido este camino con fortuna. En este sentido, la integración de sistemas será una estrategia adecuada, aunque siempre estará condicionada por la disponibilidad de los componentes intermedios específicos claves. La experiencia demuestra que en todos los sistemas existen algunos componentes que no son accesibles o lo son en unas condiciones de plazos y/o costes que impiden ser competitivos. Son componentes cuyos plazos y costes de desarrollo requieren algún cliente cautivo, que sólo puede ser la Administración.

- **Apoyo de la Administración y en particular del Ministerio de Defensa.** Las administraciones de los países son siempre los principales clientes de equipos militares. Sin su apoyo decidido no son posibles las industrias nacionales en este sector. La demanda interna no sólo permite financiar una buena parte de los desarrollos, sino que, como ya se ha indicado, avala internacionalmente los productos. Es muy difícil vender un producto que no ha sido debidamente probado por las Fuerzas Armadas propias. El nuevo contexto internacional obligará a modificar los planteamientos de este apoyo, en todo caso, su papel será básico en la planificación de la demanda y en la orientación de la oferta.

Las Fuerzas Armadas también pueden colaborar en la definición de unos requisitos que cubran las necesidades de manera ambiciosa pero realizable y en el apoyo a la realización de pruebas y evaluaciones que permitan introducir mejoras y depurar errores. Los programas conjuntos entre las empresas/centros de investigación/universidades y Fuerzas Armadas-para el desarrollo e implantación de las futuras telecomunicaciones militares son, desde este punto de vista, imprescindibles.

- **Programas de colaboración internacional.** No se puede concebir el desarrollo de una política de defensa común europea sin una política de armamento europea que en un futuro armonice sus sistemas de armas y de mando y control. Esto supone una oportunidad para la cooperación multinacional que requieren los actuales desarrollos tecnológicos, organismos de cooperación en materia de armamentos como la Agencia Europea de Armamento (EDA), pueden aportar el entorno adecuado para este tipo de actividades. Los ámbitos aquí considerados son considerados por la OTAN y la EDA como de especial interés.



- **Potenciación del mercado exterior.** La demanda interna es incapaz de satisfacer las posibilidades del sector, siendo necesario abrirse no sólo al mercado europeo, que ya es el nuestro, sino también a otros, como el sudamericano, con un innegable potencial de futuro. La política exterior y de seguridad del Gobierno no es neutral. La revisión de estas políticas y el incremento del apoyo institucional, por ejemplo a través del Ministerio de Asuntos Exteriores, son oportunidad que se debe poner a disposición de nuestra industria. La Directiva de Defensa Nacional, como ya se ha comentado, permite ser optimistas en este punto.
- **Un idioma y una cultura común.** Esta ventaja no sólo afecta al desarrollo de interfaces en castellano o a la redacción de manuales de operación y mantenimiento mucho más amigables. La facilidad de comunicación con el cliente español o sudamericano permite capturar los requisitos específicos de los clientes y crea un ambiente apropiado para el éxito de las iniciativas. La extensión del uso de nuestra lengua y cultura común es un factor muy positivo para la economía nacional en general, y en particular para los sectores ligados a las TIC's, constituyendo una herencia que todos debemos defender.
- **Incremento de las actividades de I+D+I.** A pesar de que el sector de la Defensa y la Seguridad es de los que más contribuye a la I+D+i nacional sigue siendo insuficiente. Debilidad puede convertirse en oportunidad si se toman medidas; es de lo que trata el siguiente subapartado.

7.4 Investigación, desarrollo e innovación en telecomunicaciones militares dentro del ámbito de las TIC

En España las actividades de I+D en este campo son fundamentalmente aplicadas y, en muchos casos, muy próximas al producto final. Son muy intensas y de gran calidad en ciertos campos (radiofrecuencia, proceso de señal, sistemas de proceso de información asociados, guerra electrónica, SDR, terminales para aplicaciones espaciales, etc.) pero responde más a esfuerzos puntuales que a una estrategia definida.

Se trata de investigación orientada al cliente que se está imponiendo, sobre todo en el entorno europeo, como mecanismo para asegurar su éxito comercial. Lo característico de esta forma de trabajo radica en que el cliente, en este caso las Fuerzas Armadas y de Seguridad del Estado, participan en todas las fases de los proyectos definiendo conjuntamente los requisitos; colaborando en el desarrollo mediante el seguimiento y control de las actividades; y evaluando los equipos desarrollados en entornos lo más realistas posibles. En este sentido, debe



resaltarse la importancia de disponer de infraestructuras, plataformas experimentales e, incluso, equipos especiales para la realización de pruebas. Lo que, en muchos casos, sólo puede suministrar el propio cliente. La disponibilidad de infraestructuras como el Instituto Tecnológico de la Marañosa o el INTA, entre otros muchos ejemplos, es de gran relevancia.

El fenómeno de la globalización también está afectando a la I+D+i cuya internacionalización es creciente. España participa en la oficina de investigación y tecnología de la OTAN y en varios programas conjuntos. En cualquier caso, los grandes proyectos de innovación han sido, por su volumen y duración, los grandes programas europeos basados en programas de adquisiciones de sistemas de armas.

Por otro lado las limitaciones de fondos, derivadas del elevado coste de desarrollo de los equipos, se traducen en que cada día es más frecuente que los recursos de I+D+I se empleen, en un porcentaje más elevado, en el desarrollo de equipos bajo especificaciones operativas. Incluso, los prototipos desarrollados en teóricos entornos de I+D, se convierten prototipos operativos. En muchos casos, esta situación es consecuencia de las presiones de las propias Fuerzas Armadas que, a su vez, responde a su percepción de escasez de medios para cumplir sus misiones o a los lógicos apremios por disponer de las posibilidades que le ofrece las nuevas tecnologías para aumentar la eficacia en su cumplimiento. Un síntoma claro de esta situación es el acortamiento que, en los últimos años, se está produciendo de los plazos para el desarrollo de los sistemas, con una evidente reducción de los tiempos exigidos desde su concepción a su operación en campo. Si se sigue abusando de este fenómeno, estamos condenados a una I+D+I en el sector que cada vez tendrá más de Desarrollo, menos de Innovación y casi nada de Investigación. Las consecuencias no podrán ser otras que la descapitalización tecnológica de nuestras empresas. También es cierto que es un fenómeno que se está produciendo en casi todos los sectores y en muchos países de nuestro entorno y que, en último término, responde a las limitaciones presupuestarias. Es significativo que este fenómeno este mucho más atenuado en Estados Unidos, donde su Departamento de Defensa sigue financiando investigación básica.

Un paliativo a esta tendencia son los planes directores de I+D promovidos por La Dirección General de Armamento y Material, en colaboración con los estados mayores de la Defensa y de los Ejércitos y la Armada, y elaborados con la participaron miembros de las Fuerzas Armadas, empresas del sector y universidades, donde se definen los objetivos y líneas de actuación del Ministerio en este ámbito. Los aspectos más significativos de sus contenidos son la definición de una política de I+D en Defensa y la selección de las áreas tecnológicas de interés.

Que las tecnologías y sistemas descritos en estas páginas sean consideradas con la relevancia que merecen en los próximos planes directores y en general en los planes nacionales de I+D, es condición necesaria para que las TIC, y las



telecomunicaciones en particular, tengan el nivel de desarrollo que este país se merece. Así mismo es esencial que ambas iniciativas estén coordinadas.

Por último conviene insistir en la necesidad de que el Ministerio de Defensa disponga de algunos centros de investigación propios y de una investigación propia en este campo aunque esté en parte externalizada, ya que la definición de las necesidades a medio y largo plazo no pueden surgir sólo del mundo industrial, siempre preocupado por los productos finales y el mercado. En este punto es importante destacar que en España existe una gran cantidad de recursos humanos e infraestructuras de investigación en el ámbito de las telecomunicaciones que apenas se está utilizando.



8 CONCLUSIONES Y RECOMENDACIONES

La importancia de los sistemas de telecomunicaciones en el mundo militar es innegable. La “superioridad de la información”, obtenida mediante la aplicación intensiva de las Tecnologías de la Información y Comunicaciones (TIC), es un factor fundamental para garantizar el éxito de las operaciones militares. Estas han cambiado, de tal modo que se ha pasado de un énfasis en las características “cuantitativas” de la guerra a una situación en la que los factores cualitativos (oportunidad, indetectabilidad, precisión, sostenibilidad, escalabilidad, acciones y efectos) son cada vez más importantes. Los despliegues en el exterior, en los que se centra el presente documento, no son una excepción a este hecho. Resultaría impensable, además de inviable, llevarlos a cabo hoy en día sin un fuerte apoyo TIC.

Se ha reseñado el carácter transversal de las TIC a todos los elementos y sistemas que participan en cualquier conflicto (mando y control, transporte, sistemas de armas, inteligencia, guerra electrónica...), así como su capacidad para incrementar su eficacia exponencialmente. El documento se ha centrado en las comunicaciones tácticas en el exterior, entendiendo como tales aquellas que tienen como objetivo el intercambio de información entre un gran número de unidades tácticas (plataformas y hombres) desplegadas en un área, en muchos casos muy extensa, que disponen de terminales para la transmisión de voz y datos, con objeto de optimizar las operaciones militares conjuntas. Dado que estas redes se emplean fundamentalmente en tiempos de crisis, la movilidad resulta ser un elemento esencial.

Como ha quedado patente a lo largo del documento estas tecnologías evolucionan constantemente -pocas de las tecnologías que se mencionan tenían peso hace 20 años- siendo su continua evolución lo único seguro en este campo. Esto supone que las Fuerzas Armadas necesiten un esfuerzo especial no sólo para su adquisición y modernización, sino también para la asimilación de las mismas en la doctrina vigente, la formación de su personal en su uso, etc. Incluso supone en ocasiones cambios organizativos, como es el caso de la reciente creación de mandos especializados en Ciberdefensa en el seno del Ministerio de Defensa (como puedan ser el Mando Conjunto de Ciberdefensa en el EMAD y la Dirección de Ciberdefensa en el Ejército del Aire).

También debe recordarse que las TIC no son sólo *software*, sino que como se aprecia a lo largo del documento, de hecho, involucran tecnologías *hardware* avanzadas e incluso del estado del arte en campos tales como la guerra electrónica y el procesado de la información.

No deben obviarse los condicionantes económicos que actualmente afectan a las



Fuerzas Armadas de todo el mundo. La situación actual está llevando a la reducción de las adquisiciones de sistemas de armas de última generación, incluyendo en ocasiones la reducción en el número de unidades comprometidas de determinados sistemas de armas (como ha hecho recientemente Alemania con sus helicópteros Tigre y NH-90 [1]). Por otra parte, el entorno de seguridad actual y futuro, a nivel nacional e internacional, más complejo y menos predecible que en el pasado, requiere de un creciente ritmo de preparación, y de la capacidad de responder rápida y eficazmente a numerosos desafíos, que pueden desencadenarse en forma de efectos en cascada, muy negativos en la seguridad de los Estados.

Los escenarios que se barajan para el futuro hacen imprescindible que cualquier nación que se precie de ser tecnológicamente avanzada necesite dominar estas tecnologías. No sólo se está comprobando que la ciberguerra es una posibilidad real de efectos potencialmente devastadores para los sectores productivos de cualquier país, sino que enviar tropas mal equipadas en cuanto a TIC a cualquier escenario de conflicto supone un riesgo demasiado elevado. La obsolescencia de los sistemas disponibles hace una década, junto a la cada vez mayor capacidad de los sistemas disponibles comercialmente, hacen que sea necesario hacer un esfuerzo si se quiere contar con la tecnología adecuada para poder operar en un despliegue en el exterior. Puede asumirse que cualquier tecnología de prestaciones comparables a la comercial podrá estar a disposición de cualquier oponente potencial.

Las Fuerzas Armadas deberían contar con capacidad para poder orientar a la industria del sector sobre sus necesidades tecnológicas. La situación actual hace incluso más evidente que estas deban priorizarse. Por ejemplo, las recientes declaraciones del JEMAD, Almirante General Fernando García Sánchez, a la revista *Atenea* el 13 de marzo del 2013 sobre la importancia futura de la ciberdefensa y las tecnologías relacionadas con los vehículos no tripulados apuntan que estas podrían considerarse prioritarias³. Sin embargo, resultaría muy conveniente contar con la capacidad de producir sistemas completos, aunque no se lleguen a fabricar por razones económicas. Esto permitiría mantener lo que podría denominarse como “soberanía tecnológica”, evitando la total dependencia del exterior para la Defensa Nacional. También permitirá, por ejemplo, evitar restricciones al uso o a la comercialización de determinados componentes incluidos en los sistemas de armas comercializados por las empresas españolas derivadas de las condiciones de su adquisición. De hecho, la tendencia en algunos países está pasando por mantener un cierto grado de la citada soberanía tecnológica en los sistemas que afectan directamente a la seguridad nacional -como es el caso de la iniciativa *Trusted Foundry* de EEUU [3]. La relevancia de la existencia de una industria propia de

³ En una entrevista anterior en un medio de difusión nacional [2] ya indicó que habría que “conseguir aquellas capacidades emergentes necesarias para desarrollar nuestros planes de contingencia en el siglo XXI como nuevas capacidades de mando, control, comunicaciones y gestión de la información, medios conjuntos de inteligencia, vigilancia y reconocimiento, y capacidades de ciberdefensa”



Defensa para el mantenimiento del nivel tecnológico de España es indiscutible. El volumen de trabajos de alta cualificación que esta genera no es fácil de conseguir en otros sectores más tradicionales y las sinergias con otra industria relacionada (mediante las tecnologías duales) ayudarán sin duda a mejorar la competitividad de la misma.

Para mantener la capacidad de fabricar sistemas TIC de Defensa no es necesario que la industria comercialice todos los sistemas posibles, sino que bastaría con que se desarrollaran trabajos al más alto nivel, es decir, abarcando la capacidad de diseño y el know-how de dichos sistemas, en las áreas que no resulten rentables para la industria. Esto permitiría contar con suficientes recursos humanos (ingenieros, técnicos) y materiales (maquinaria, software específico) para poder, en su caso afrontar nuevos retos. En este sentido, tampoco debería olvidarse que el sector de las telecomunicaciones por su propia naturaleza abarca tecnologías de carácter emergente que requieren una fuerte especialización.

Por lo complejo de los sistemas y las tecnologías involucradas, resulta necesario alinear los instrumentos de apoyo a la innovación en áreas de interés para la Defensa, como puedan ser programas como COINCIDENTE con los esfuerzos de I+D realizados por las empresas. No puede enfatizarse lo suficiente que en este proceso lo primordial es apoyar los desarrollos que cubran necesidades de las Fuerzas Armadas y que no puedan recibir apoyo por otras vías, ya que en caso contrario, quedarían sin cubrir, al menos mediante tecnología nacional. Aunque no deba perderse de vista la posibilidad de realizar desarrollos de tecnología dual, estos pueden y deben buscar financiación tanto en el sector militar como en el civil, además de tener un mayor mercado potencial.

La colaboración de las Fuerzas Armadas en el desarrollo de tecnología por parte de la industria nacional no podría ser más importante. El que unas Fuerzas Armadas empleen un determinado material es garantía para otros ejércitos de su fiabilidad. No obstante y esto no debe olvidarse, para ello el sistema deberá cumplir los más altos estándares de calidad y ser comparable al resto de sistemas de su gama disponibles. En cualquier caso, cualquier otra opción, relega el proceso de internacionalización en el que se encuentra inmerso el sector a la competencia en mercados de “segunda fila” (básicamente naciones especialmente atrasadas que no puedan permitirse algo mejor). Dado el crecimiento de las exportaciones de armamento de países como China, que ha llegado ya a estar entre los cinco primeros exportadores del mundo [4], el modelo basado en la competencia en costes (de productos de gama media) corre el riesgo de encontrarse con una competencia tal que lo haga inviable y aboque a la industria nacional a su desaparición.

En este sentido, una de las mayores ayudas que puede aportar el propio Ministerio es mantener unos elevados niveles de rigor en la adquisición del material, evitando



la compra de sistemas de calidad deficiente, que no cumplan requisitos o que se encuentren muy por encima de su precio real. Esto obligará a que realmente las empresas involucradas sean competitivas y eficientes, contratando la mano de obra especializada que sea precisa y contribuyendo por tanto a mantener un elevado nivel tecnológico y conocimiento en el país.

A nivel europeo, merece la pena señalar que la propia jefa de la diplomacia europea, Catherine Ashton indicaba recientemente [5] que será necesario cooperar en la adquisición y mantenimiento de capacidades por parte de las Fuerzas Armadas europeas o se correrá el riesgo de perderlas con las consecuencias que ello traería para Europa, que incluirían la imposibilidad de contribuir a ningún tipo de misión de paz e incluso una menor capacidad defensiva de los Estados Miembros de la UE. Dada la importancia de las TIC en las misiones en el exterior tal vez podría valorarse esta alternativa en caso de que sea imposible adquirirlas mediante un esfuerzo exclusivamente nacional.

Por último, como puede verse a lo largo del presente documento la velocidad con la que aparecen nuevas tecnologías es vertiginosa y actualmente se están produciendo cambios socioeconómicos de envergadura que afectan también al sector de la Defensa. En el Grupo de Trabajo de Defensa permaneceremos atentos a los continuos cambios tecnológicos y en función de las novedades que se produzcan habilitaremos los canales convenientes hacia nuestros colegiados y la sociedad en general para su comunicación.



9 REFERENCIAS

Castro J.C. "Jornada sobre la Contribución de los Programas de Armamento y Material del Ejército de Tierra al Planeamiento por Capacidades de la Defensa" Fundación Círculo de Tecnologías para la Defensa y la Seguridad (abril 2012).

Chan S. "Shared Spectrum Access for the DoD". IEEE Communications Magazine (junio 2007).

Frederick H. Raab, Robert Caverly, Richard Campbell, Murat Eron, James B. Hecht, Arturo Mediano, Daniel P. Myer, and John L. B. Walker. "HF, VHF, and UHF Systems and Technology". IEEE Microwave Theory and Techniques (marzo 2002).

IEEE "Future Tactical Military Communications Systems Seminar" (junio 2010).

IEEE "Taxonomy v. 1.01" (enero 2009).

IETF. "Mobile Ad-hoc Networks (MANET)." The Internet Engineering Task Force, <http://www.ietf.org/html.charters/manet-charter.html>.

JED - Journal of Electronic Defense. Varios artículos:

- "US Helicopter EW" (marzo 2012).
- "ADCs and DACs in EW: Far More Than Bit Players" (febrero 2012).
- "SIGINT and Direction Finding Antennas" (agosto 2011).
- "TWTs and Beyond: Putting More Power into EW" (mayo 2011).

Joaquín Moreno. "Bastionar una DMZ". Security art work (2009).

Ministere de la Defense de la France "Strategic Plan for R&T in Defence and Security" (enero 2009).

Ministerio de Defensa de España "Monografía CESEDEN Tecnología y Fuerzas Armadas" (febrero 2007).

Mitola J. "The Software Radio Architecture". IEEE Communications Magazine (mayo 1995).

NATO "Affordable Defence Capabilities for Future Missions" (febrero 2010).

NATO C3 "Classification Taxonomy Baseline 0.95" (mayo 2012).

NATO-EU "Cooperation on C4ISR Capabilities for Crisis Management" (noviembre 2011).



NATO MC 593/1 Draft Version “Minimum level at Command and Control (C2) Services in Support of Joint NATO Operations in a Land Based Environment” (enero 2012).

NATO RTO-MP-IST-042 “Coalition C4ISR Architectures and Information Exchange Capabilities” (diciembre 2005).

NATO RTO-MP-IST-054 “Military Communications” (diciembre 2006).

NATO RTO-TR-IST-067 “Technical Communications in Urban Operations” (septiembre 2010).

Moffatt C.D. and Lilley R.D. “High-Data-Rate, Network Radio for Wireless Communications in Military Environments”. IEEE Military Communications Conference. MILCOM (octubre 2007).

Perlman B., Laskar J., and Lim K. “Fine_Tunning Commercial and Military Radio Design”. IEEE Microwave Magazine (agosto 2008).

Prieto A. “Jornada sobre Radio definida por software – SDR”. Fundación Círculo de Tecnologías para la Defensa y la Seguridad (marzo 2009).

Scheers B., Mahoney A. and Akermark H. “A Realistic Roadmap for the Introduction of Dynamic Spectrum Management in Military Tactical Radio Communication”. Military Communications and Information Systems Conference (octubre 2012).

UK MoD “Defence Technology Strategy for the demands of the 21st century” (mayo 2011).

US DoD “C4ISR Architecture Framework” (julio 2010).

US DoD “Strategic Spectrum Plan” (febrero 2008).

UN “Lessons learned in Peacekeeping Operations” (septiembre 2012).

[1] <http://www.businessweek.com/news/2013-03-15/germany-cuts-eads-military-chopper-order-while-adding-navy-model>

[2] ABC, 4 de marzo de 2012

[3] <http://www.trustedfoundryprogram.org/>

[4] <http://www.rtve.es/noticias/20130318/sexta-ano-consecutivo-aumento-venta-armas-mundo/619580.shtml>

[5] EFE, 22 de marzo de 2013



colegio oficial
ingenieros
de telecomunicación

Almagro, 2 28010
Madrid

Tel.: 91 391 10 66
Fax: 91 319 97 04
e-mail: coit@coit.es
web: www.coit.es