El papel de las TIC en los Sistemas para la Seguridad y la Defensa

Félix Pérez Martínez, Catedrático de la ETSI de Telecomunicación de la UPM

Las características de las TICs -ruptura de las barreras espaciales y temporales, flexibilidad y adaptabilidad, interactividad e inteligencia, reducción de costes y horizontalidad, entre otras- las convierten en factores multiplicativos de las actividades humanas, simplificando e incrementando la productividad de los procesos. Esto explica su potencial transformador y su protagonismo en el avance de muchos sectores productivos, a los que ha arrastrado a un progreso de resultados impensables hace sólo unos años.

El sector de la Defensa y Seguridad, que fue el motor inicial de estas tecnologías y uno de los elementos básicos de su actual desarrollo, también está sometido a cambios estructurales derivados de su masiva introducción. En este artículo se reflexiona sobre las razones de ello y como las TICs están transformando a las Fuerzas Armadas y de Seguridad de los países avanzados.

Los sistemas de Seguridad y Defensa del siglo XXI

Los nuevos sistemas deberán enfrentarse a sofisticadas amenazas y al aumento de la capacidad de las armas, en términos de alcance y precisión. Asimismo, combatirán con otras amenazas, como las armas de destrucción masiva o los atentados indiscriminados, no necesariamente sofisticadas y por ello de relativamente fácil acceso. Todo ello está obligando replantearse la estructura y modo de operación de los sistemas de Seguridad y Defensa del siglo XXI. De hecho es un camino ya iniciado en la última década del pasado milenio y tiene por objeto la satisfacción de los siguientes requisitos:

– **Sencillez** para los operadores. La gran cantidad, diversidad y complejidad de las informaciones presentes en el escenario impide que el operador tenga tiempo para analizarlas con detalle. Su única interfaz será un teclado con números y funciones preprogramadas y una pantalla sintética que le presenta el resultado de complejos procesos – la mayor

parte de ellos automáticos - de adquisición y tratamiento de una información que varía en origen a un ritmo del orden de 10^9 bits/segundo, para reducirla a los 10 o 20 bits/s que cada operador es capaz de asimilar.

- **Rapidez**. En un conflicto moderno las acciones se desarrollan con extremada rapidez y en muchas ocasiones las decisiones deben tomarse casi en tiempo real y por personas muy alejadas de los lugares donde están desplegados las unidades y los equipos.
- **Integración** con otros sistemas. Las decisiones requieren el conocimiento de informaciones adicionales a los que se está obteniendo el sistema – datos obtenidos por otros sistemas, datos almacenados de inteligencia y logísticos, etc. -, por lo que no pueden trabajar aisladamente.
- **Interoperabilidad**. La diversidad de situaciones y misiones exige equipos capaces de operar con otros, propios o de los aliados, en diferentes configuraciones que permitan su utilización flexible para optimizar su eficacia. Necesidad que cada día es más perentoria por el elevado coste de estos sistemas.
- **Seguridad.** Mediante el empleo de técnicas de autentificación, corrección de errores y cifrado debe asegurarse la calidad de las informaciones manejadas así como que nadie no autorizado accede al sistema. También debe garantizarse que la información que viaja por sus redes no es conocida o modificada por personas u organizaciones ajenas.
- **Redundancia** de las informaciones y redes. La probabilidad de fallos disminuye drásticamente si se manejan datos con orígenes diferentes y se transmiten por diferentes redes de comunicaciones.

"Los nuevos sistemas deberán enfrentarse con otras amenazas, como las armas de destrucción masiva o los atentados indiscriminados, no necesariamente sofisticadas y por ello de relativamente fácil acceso"

Por otro lado, el modo de operación de estos sistemas será radicalmente distinto al de la mayoría de los desplegados en la actualidad. Los nuevos sistemas serán de estructura muy descentralizada pero de decisión centralizada, donde la mayor parte de las funciones están automatizadas dejando a los operadores labores fundamentalmente de mantenimiento, supervisión y decisión. Paradójicamente, la preparación técnica de estos últimos debe ser muy superior, pues su labor, a diferencia de lo que ocurría hace años, tiene muchos más componentes "científicos" que "artísticos": su formación está mucho menos basada en la experiencia previa en el uso de los sistemas que en sólidos conocimientos científico-técnicos.

Estructura de los nuevos sistemas para la seguridad y la defensa

En casi todos los actuales sistemas es fácil identificar los siguientes elementos:

- **Sensores.** Capaces de detectar y determinar los parámetros esenciales de los objetivos (posición, velocidad, capacidad de fuego...) así como de analizar otras señales del espectro electromagnético. Trabajan en las diferentes bandas: radiofrecuencia (radares y receptores pasivos), electroópticas (cámaras térmicas y radares láser), acústicas etc, complementando las características de cada una de ellas. Asimismo, están dotados de elementos de protección electrónica capaces de enfrentarse con perturbadores y otras acciones de Guerra Electrónica cada vez más sofisticadas. Por último, cada cierto tiempo, el sensor debe enviar sus datos a los centros de control o recibir órdenes.
- **Redes de comunicación**
  La salida de los sensores debe ser enviada a otros elementos del sistema de más alto nivel y estos deben enviar a los sensores sus ordenes de trabajo. En función de la calidad de la red, que se incrementa en la medida que interconecta elementos de mayor nivel, se utilizarán uno o varios medios físicos. En el futuro, se duplicarán casi todas las redes para asegurar su inmunidad a fallos.
- **Centros de mando y control**
  Reciben los datos de numerosos sensores y atienden las peticiones de órdenes de las diferentes unidades. Además, están interconectados con otros centros de mando y control. Su hardware es de elevadas prestaciones - en términos de rapidez, fiabilidad y disponibilidad - y el software que incorporen es multitarea con una amplia utilización de nuevas téc-

"La preparación técnica de los operadores estará menos basada en la experiencia previa en el uso de los sistemas y más en sólidos conocimientos científico-técnicos"

nicas de fusión de datos e inteligencia artificial. Los centros se estructuran de manera distribuida pero perfectamente coordinados entre sí, con una delimitación clara de responsabilidades.

– **Subsistemas de Guerra Electrónica**
En muchos casos los sistemas estarán dotado de capacidad de ataque y defensa electrónica, lo que requiere un conocimiento muy profundo de los sistemas objeto de su acción. De hecho, en el futuro –ya ocurre ahora en muchos casos– será necesario conocer el modo concreto en que están trabajando en cada momento las distintas amenazas, dado que están dotadas de técnicas para optimizar su eficacia perturbadora y oponerse a los ataques electrónicos. Esto implica dotar a estos subsistemas de adaptabilidad, inteligencia y comunicaciones (por las que recibirán datos obtenidos de otros sistemas, por ejemplo, de sensores y sistemas de inteligencia electrónica).

La conclusión que se extrae de esta breve descripción es que los requisitos de los nuevos sistemas asociados a las aplicaciones de Seguridad y Defensa son imposibles de obtener sin la conjunción de las tres tecnologías básicas: electrónica, informática (software) y comunicaciones, fuertemente imbricadas entre sí. La clave del éxito de estos sistemas estará, por tanto, en disponer de los sensores, comunicaciones y sistemas de información más adecuados a los objetivos perseguidos, junto a la correcta formación de los operadores y mandos, todo ello enmarcado en nuevas doctrinas y estructuras organizativas adaptadas a las nuevas características de los conflictos y de los medios disponibles para su resolución.

Investigación, Desarrollo e Innovación en TICs en el ámbito de la Defensa y Seguridad

En pocos años hemos pasado de un escenario de conflicto caracterizado por la existencia de dos grandes bloques políticos respaldados por una capacidad militar en constante crecimiento, a otro en el que las amenazas no se derivan de una gran potencia militar sino de un enemigo disperso y extendido, poco numeroso, pero con una gran capacidad de aprovechar las debilidades de la una sociedad tan compleja como la que nos ha tocado vivir. En la nueva situación no hay un enemigo bien identificado que pretende destruir objetivos claramente definidos. Lo que cabe esperar es que los ataques se realicen contra objetivos civiles indiscriminados, incluyendo las infraestructuras básicas que soportan nuestro modo de vida: aeropuertos, sistemas de comunicaciones, medios de información etc. Unos ataques que no requieren grandes medios y, lo que es peor, una buena parte de ellos pueden obtenerse con relativa facilidad.

Sin embargo, sería un error pensar que, la superioridad tecnológica sobre la amenaza hace innecesario el desarrollo de nuevas tecnologías. La Defensa y la Seguridad seguirán siendo voraces consumidores de TICs, generando una significativa actividad económica, aunque cambiarán algunas prioridades y, a medio plazo, no será tan importante el desarrollo de nuevas tecnologías como la aplicación eficiente de las ya disponibles.

Características de la I+D+i en Defensa

En España la Investigación realizada en este campo es fundamentalmente aplicada y muy próxima al producto final. Entre otras, presenta las siguientes características:

– **Investigación orientada al cliente**. Este tipo de investigación 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 las de Seguridad del Estado, participa en todas las fases de los proyectos: definiendo los requisitos a partir de unas necesidades establecidas, colaborando en el desarrollo mediante el seguimiento y control de las actividades y evaluándolos en entornos lo más realistas posibles.

– **Internacionalización de la I+D+i**. Los grandes proyectos de innovación han sido y serán, por su volumen y duración, los grandes programas europeos basados en programas de adquisiciones de sistemas de armas.

"Si los recursos de I+D+i se emplean sólo en el desarrollo de equipos bajo especificaciones operativas, la consecuencia será la descapitalización tecnológica de nuestras empresas"

– **Tendencia al Desarrollo**. La realidad indica que 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. Un síntoma claro de ésta situación es el acortamiento que 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.

La formación en TICs en el ámbito de la Defensa y la Seguridad

En todos los países la enseñanza militar y policial tradicional se ha caracterizado por su autarquía, de modo que los conocimientos, la preparación del profesorado, las técnicas de formación, la documentación empleada etc., se han generado básicamente desde sus propios ámbitos. Naturalmente, hay numerosas excepciones a esta afirmación y pueden argumentarse aportaciones directas desde el sistema educativo general a la educación militar, pero ello no la invalida, como lo demuestra la existencia de una organización de la enseñanza militar de gran tradición en todos los niveles.

La profesionalización de las Fuerzas Armadas, con la consiguiente reducción de efectivos, plantea un problema inmediato de recursos humanos en su doble vertiente: no habrá suficientes alumnos y profesores para mantener la actual estructura. Sin embargo, existe otro problema menos explícito pero, posiblemente, a medio plazo más importante: el efecto que la introducción de las TIC produce en los contenidos y técnicas de formación.

Estas tecnologías no sólo "impregnan" los actuales sistemas de armas y de mando y control, también han demostrado sus posibilidades en otra amplia gama de aplicaciones, tales como la gestión virtual de organizaciones, simuladores y entrenadores, teleducación, mantenimiento de equipos... Su introducción exige modificar el "saber hacer" de los equipos humanos que, como ya se ha comentado, tendrá que basarse más en conocimientos sólidos que en la práctica.

Ningún sistema de enseñanza puramente militar será capaz de formar adecuadamente en las TIC (afirmación que posiblemente pueda extenderse a otros campos) y la clave del éxito no es otra que la imbricación de los sistemas de enseñanza militar y civil en todos los niveles, aprovechando al máximo los recursos disponibles. Además, no hay que olvidar que la convivencia entre militares y civiles que supone es un instrumento más para incrementar la "cultura de Defensa" en nuestro país, algo que, con sobrados motivos, se reclama desde el ámbito militar.

Conclusiones

Inevitablemente nos esperan décadas en que los sistemas para la Defensa y la Seguridad serán cada vez más sofisticados, costosos y eficaces, cuya correcta operación requerirá cambios constantes, tanto en la organización y doctrinas de los Ejércitos, como en la formación de sus recursos humanos. La gestión de todo ello es uno de los retos a que deberán enfrentarse nuestras autoridades civiles y militares.

Especial atención deberá dedicarse a cómo este proceso afectará al sector industrial nacional, cuya supervivencia requiere una política propia por parte de la Administración para afianzar la base tecnológica y promocionar las empresas del sector, dotándolas de unas dimensiones y capacidades compatibles con el nivel industrial de nuestro país y las necesidades de la Defensa. No hay que olvidar el efecto difusor de este sector en la formación del tejido industrial español y sus consecuencias sobre el empleo.

Afortunadamente, la industria y los organismos públicos de investigación españoles disponen de la base científica y técnica necesaria para hacer frente a los nuevos retos en materia de seguridad. ◆