

Tecnologías disponibles para la Seguridad

El atentado terrorista del pasado 11 de Septiembre ha significado la confirmación manifiesta de un cambio que venía percibiéndose en el terreno de la defensa y la seguridad desde hace algún tiempo. En el transcurso de pocos años, hemos pasado del escenario de confrontación de grandes bloques políticos a otro en el que las amenazas ya no están asociadas a una gran potencia militar sino a un enemigo organizado en pequeños grupos, con una enorme autonomía y con una gran agilidad. Lo más inquietante de la nueva situación es que ya no luchamos ahora contra un eventual ataque de un enemigo bien identificado empleando armas de destrucción masivas contra objetivos claramente definidos, sino contra el riesgo mucho más insidioso de ataques contra objetivos civiles, que constituyen el corazón de sistemas clave para el sostenimiento de la actividad económica de los países (i.e. aviación comercial, sistema financiero), en definitiva contra algunos de los símbolos de nuestro *estado del bienestar*. Además, este tipo de acciones no requiere un gran despliegue de medios materiales, lo que dificulta enormemente su detección y la prevención de los mismos. Por otra parte, el fenómeno de la globalización ha permitido la aparición de un nuevo modelo de terrorismo en red, altamente tecnificado, y que puede originarse y golpear en cualquier lugar del mundo.

En este nuevo escenario, cambia el paradigma de defensa contra las amenazas externas. De hecho, cabe decir que en un mundo globalizado todas las amenazas han dejado de ser externas, y que nos enfrentamos al enemigo en casa, luchando dentro de nuestras fronteras y, en muchos casos, con nues-

• **Luis Mayo**

Director General (CEO). Grupo Tecnológico e Industrial GMV, S.A.

tras propias armas en cuanto a tecnología. Planteado en estos términos, el problema puede no estar tan ligado al desarrollo de nuevas tecnologías como a la aplicación eficiente de las tecnologías disponibles para hacer frente a las amenazas insurgentes en este nuevo escenario. O en otros términos: el problema no es tanto de I+D, investigación y desarrollo, como de D+I, desarrollo e innovación; es decir, el nuevo desafío es definir nuevos procesos que nos permitan aprovechar de forma óptima las tecnologías disponibles para combatir al enemigo que ha surgido en los últimos años tras la descomposición del bloque del Este y la aparición de los movimientos terroristas universales.

¿Cómo podemos poner las tecnologías existentes al servicio de las estrategias necesarias para enfrentarnos a los nuevos escenarios de seguridad? Como se ha puesto de manifiesto en los recientes acontecimientos de la guerra de Afganistán, la estrategia de defensa ya no puede plantearse en términos de justa revancha ("retaliation"). Los enemigos no poseen objetivos que merezcan el coste de los medios necesarios para destruirlos en la mayoría de los casos. Así pues, el planteamiento que debe hacerse es radicalmente diferente. En primer lugar, es necesario prevenirse contra este tipo de ataques, es decir, disponer de información continua, precisa y fiable sobre los posibles planes de estos grupos. En segundo lugar, es preciso proteger los activos críticos contra estos ataques.

Pues bien, hace años que existen tecnologías que pueden contribuir en gran medida a estos objetivos. Un buen ejemplo de ello son las tecnologías espaciales. En la actualidad estas tecnologías encuentran aplicaciones en el sector de la defensa y la seguridad de forma que casi podría calificarse de rutinaria en diversos ámbitos dentro del mundo de la defensa y la seguridad. Por ejemplo, se dispone de satélites de observación y vigilancia, tanto en lo que se refiere a la obtención de imágenes en diferentes bandas del espectro electromagnético (óptica, IR, MW - i.e. SAR -) como en lo que se refiere a la escucha de telecomunicaciones. Ciertamente, puede discutirse la capacidad de nuestro país para construir por sí solo uno de estos sistemas, pero no es menos cierto que nuestra industria participa en el desarrollo de este tipo de sistemas y que nuestros cuerpos de defensa y seguridad tienen acceso a este tipo de información. Baste para ello recordar la participación española en el satélite espía Helios. Es también evidente que los satélites proporcionan una alternativa muy interesante para proteger una infraestructura crítica desde el punto de vista social, político y económico para nuestra sociedad: la de telecomunicaciones. Es palpable como tras el 11 de septiembre, el gobierno de los EEUU ha incrementado su uso de las telecomunicaciones por satélite entre otros motivos para disponer de una infraestructura alternativa a otros medios más susceptibles de ser atacados (interferidos, destruidos o de cualquier otra forma) por un grupo terrorista. Es obvio que un satélite estacionado en órbita a 36.000 km de altura resulta mucho menos vulnerable que un nodo de comunicaciones en tierra. También estas tecno-

El problema no es tanto de disponibilidad de las tecnologías como de una aplicación innovadora a los nuevos problemas planteados en el escenario actual de seguridad y defensa

logías están disponibles en nuestro país básicamente, si bien es evidente que no resulta rentable su explotación comercial en un mercado ampliamente globalizado como es el espacial. Algo parecido sucede con las tecnologías de posicionamiento y sincronización de tiempo por satélite, que pueden resultar vitales a la hora de proteger infraestructuras móviles, proporcionando información precisa sobre su localización en cada instante de modo que puedan protegerse adecuadamente contra intentos de toma de control por parte de amenazas externas.

En realidad, las tecnologías espaciales básicas están ampliamente disponibles en Europa, y la industria española ocupa un papel de cierta relevancia en el tejido industrial europeo en este sector, encontrándose plenamente integrada en los movimientos de concentración que se han iniciado en este sector desde hace algunos años y ocupando posiciones de liderazgo en algunas tecnologías críticas para estos sistemas, como es el caso de GMV, que desde hace años es uno de los principales suministradores de sistemas de control en tierra para satélites y misiones espaciales. El problema pues no es tanto de disponibilidad de las tecnologías como de una aplicación innovadora de las mismas a los nuevos problemas planteados en el escenario actual de seguridad y defensa en términos de:

1) Velocidad de respuesta a las amenazas.

Si bien es cierto que las tecnologías necesarias para la defensa contra estas nuevas amenazas están disponibles, no es menos cierto que lo están también en gran medida para el enemigo. Por ejemplo, un pequeño grupo de expertos, con una infraestructura muy limitada podría lanzar un ataque mediante virus a través de la red contra instituciones críticas para nuestra sociedad. Es necesario tener una gran capacidad de respuesta para detectar rápidamente estas actuaciones y responder a las mismas, lo que requiere posiblemente una forma diferente de cooperación entre los organismos de seguridad, los expertos indus-

triales y los organismos públicos de investigación.

2) Disponibilidad de soluciones alternativas: no pueden confiarse los sistemas e infraestructuras críticas a una única solución tecnológica. Debe asegurarse la disponibilidad de alternativas con tecnologías claramente diferenciadas que permitan transferir la operación de infraestructuras críticas de una a otra de forma rápida y sencilla. Por ejemplo, en este momento la tecnología de posicionamiento y sincronización depende grandemente de una única fuente de información: GPS; es vital disponer de un sistema alternativo que mejore la robustez frente a posibles ataques que puedan inhabilitar el sistema temporalmente.

3) Aprovechamiento del conocimiento existente para desarrollar rápidamente nuevas soluciones a nuevos problemas. En definitiva se trata de combatir al enemigo con sus propias armas: las de innovar con las tecnologías disponibles para buscar nuevas formas de contrarrestar las amenazas basadas en esas mismas tecnologías.

4) Por último, es necesario aumentar la capacitación tecnológica del usuario, es decir, de los operativos de las fuerzas de seguridad y defensa del Estado. En muchos casos, la utilización óptima de los medios y tecnologías disponibles dependen en gran medida del conocimiento de estos sobre las posibilidades ofrecidas por los sistemas proporcionados por la industria. Con todo, no debe cuestionarse

la necesidad del desarrollo de nuevas tecnologías. Por el contrario, es evidente que este es un elemento crítico a la hora de mantener la presente asimetría de medios con respecto al nuevo enemigo, que difícilmente puede tener los recursos necesarios para equilibrar la balanza en este sentido. Hay que mantener un esfuerzo continuo en este campo de modo que pueda mantenerse una ventaja "competitiva" sobre las nuevas amenazas que surgen en el escenario modificado de estrategia y seguridad en que nos encontramos. Y para ello, es necesaria la inversión en el desarrollo de nuevas tecnologías de comunicaciones, y en la incorporación de las tecnologías nacientes (p.ej. IP version 6, VPN, etc) a los sistemas de defensa y seguridad. Sin embargo, este esfuerzo resultará baldío si no se trasladan las tecnologías existentes a productos y procesos capaces de mejorar nuestra capacidad de respuesta frente a las nuevas amenazas de una forma innovadora.

La industria y los organismos públicos de investigación españoles disponen de la base científica y técnica necesaria para los hacer frente a los nuevos retos en materia de seguridad. Hemos tan sólo de encontrar la forma de explotar estas capacidades de forma eficiente antes de que el enemigo descubra como explotar nuestras carencias.



No. de transpondedores en uso en 2001 en EEUU

