ieee.es
Instituto Español de Estudios Estratégicos

Documento
Análisis

57/2016 14 septiembre de 2016

David Ramírez Morán

Afrontando la aplicación de tecnologías a defensa y seguridad

Afrontando la aplicación de tecnologías a defensa y seguridad

Resumen:

El rápido avance tecnológico que se está produciendo en el mundo civil contrasta con un entorno de defensa y seguridad en el que las políticas nacionales e internacionales y las dificultades presupuestarias derivadas de la crisis económica han dado lugar a una drástica reducción de su actividad. Además, este entorno ha propiciado un modelo de desarrollo fundamentado principalmente en las tecnologías de uso dual, que en muchos casos se traduce en adaptar las soluciones civiles a los usos y características específicas de un entorno tan particular como es el de la defensa y la seguridad. A la hora de implantar las tecnologías en los campos de defensa y seguridad, hacer frente a los nuevos riesgos que surgen o contar con los profesionales necesarios para el desarrollo, mantenimiento y aplicación de estas tecnologías aparecen nuevos problemas directamente asociados a este nuevo modelo.

Abstract:

The fast technological advance that is taking place in the civilian world contrasts with a defence and security environment where the national and international policies as well as the budgetary difficulties related to the economic crisis have given place to a reduction of its activity. Besides, this environment has promoted a development model based mainly on dual use technologies that, more often than not, translates into the tailoring of civilian solutions to the specific uses and characteristics of an environment as particular as the defence and security is. At the time of implanting these technologies in the fields of defence and security, facing the new risks enabled by them or enrolling the professionals required to develop, maintain and apply these technologies new problems arise directly related to this new model.

Palabras clave:

Tecnología, uso dual, seguridad, defensa.

Keywords:

Technology, dual use, security, defence.

Introducción

Un entorno seguro requiere que las soluciones utilizadas para hacer frente a las nuevas amenazas que van surgiendo sean flexibles y escalables a los nuevos escenarios de riesgo. Para ello es necesaria una investigación continua que paulatinamente encuentra crecientes problemas para conseguir financiación, especialmente cuando el producto a desarrollar es específico para el campo de la defensa. Los presupuestos de defensa de los países, y particularmente las inversiones destinadas al desarrollo y adquisición de nuevos sistemas, se han visto drásticamente reducidos con respecto a los de hace una década. En contraste, las tecnologías no han dejado de evolucionar desarrollando productos que, aplicados en el contexto de la seguridad y la defensa, pueden suponer una superioridad tecnológica, ya sea con fines de ataque o de defensa, derivados de las nuevas aplicaciones civiles que se están desarrollando.

Ante los nuevos vectores de ataque asociados a las tecnologías es necesario desarrollar los mecanismos de defensa con los que poner freno a su efectividad. Así mismo, a la hora de aplicar estos mecanismos es necesario evaluar las consecuencias que pueden tener sobre los usos civiles de esas mismas tecnologías para evitar efectos colaterales, lo que puede limitar la capacidad de defensa ante este tipo de amenazas.
Conseguir los profesionales necesarios para desarrollar o adaptar estas tecnologías al mundo de la defensa y la seguridad también supone un reto ante la competencia que supone el panorama industrial dirigido al mercado civil de, precisamente, las mismas tecnologías que se están utilizando para la defensa y la seguridad.

Tecnologías de uso dual

Internet, las microondas y el sistema GPS de posicionamiento global por satélite han sido ampliamente utilizados como ejemplos de tecnologías desarrolladas con fines militares que, una vez trasladadas al mundo civil, dieron lugar a infinidad de nuevas aplicaciones que han supuesto innumerables puestos de trabajo. Del mismo modo, la evolución tecnológica de estas soluciones con la generalización de su uso en el mundo civil, ha dado lugar a que se priorizaran los intereses comerciales frente a las necesidades de seguridad y defensa.

Cuando las capacidades de los sistemas militares se ven superadas por las que proporcionan los sistemas civiles de la zona, se puede dar la situación de que, en pos de la eficiencia, el personal desplegado considere emplear las infraestructuras civiles disponibles para contar con esas capacidades que todavía no proporcionan los sistemas militares. En el pasado ya se han producido situaciones en las que estas prácticas se han convertido en auténticos riesgos tanto para la integridad del personal como para el correcto desarrollo de las operaciones. Estos sistemas son más vulnerables a escuchas por terceros o a la obtención de información a partir de metadatos o de la información compartida por la red, que pueden dar al traste con el efecto sorpresa con el que se cuenta en algunos casos para el éxito de una operación.

Las elevadas prestaciones de los sistemas civiles y la facilidad con la que estas tecnologías están permeando en la población inducen una tendencia a implantar estos sistemas en entornos para los que no han sido diseñados. Como ejemplo, una afirmación que se repite con frecuencia en el entorno de los profesionales de la seguridad de internet es que en su diseño inicial la seguridad no era uno de los principios básicos y que ésta se ha tenido que ir introduciendo mediante modificaciones sujetas a las limitaciones de la propia tecnología. Se destaca así el contraste existente entre lo que puede proporcionar la tecnología y lo que se espera de ella bajo los nuevos escenarios en los que se desea aplicar.

Actualmente el paradigma está cambiando hacia una política de seguridad por diseño en la que la propia seguridad es un requisito más de los sistemas. El entorno de defensa y seguridad presenta especificidades que pueden desviarse de aquellas que se dan en las soluciones comerciales. Para que sean tratadas correctamente es necesario el desarrollo de tecnologías específicas que requieren una labor de investigación y desarrollo cuyo retorno de la inversión solo va a producirse dentro del contexto de la defensa y seguridad, salvo que la solución obtenida suponga una ventaja competitiva que motive la implantación de solución en aplicaciones civiles.

Implantando seguridad

La seguridad de la población requiere que se implanten medidas y límites al uso de las tecnologías. A este fin, es habitual hacer acopio de las medidas de seguridad que se han aplicado en otros entornos y evaluar cuáles pueden ser de aplicación a las nuevas tecnologías. Sin embargo, las características de la nueva amenaza pueden hacer que esas soluciones que previamente habían funcionado no proporcionen los resultados esperados al ser aplicadas a las nuevas tecnologías. Los drones e internet son dos casos paradigmáticos donde la aplicación de soluciones heredadas de otros campos se han mostrado manifiestamente insuficientes o inadecuadas para hacer frente a la amenaza.

Una característica común a las amenazas tecnológicas a día de hoy es la dificultad de atribución.

En el caso de internet, son múltiples las técnicas que permiten ocultar la identidad del atacante. Desde sistemas de anonimización específicos como TOR y otras VPN existentes, hasta el uso de *botnets*, que son conjuntos de ordenadores que han sido infectados por virus y que pasan a ser la plataforma que los atacantes pueden utilizar para lanzar ataques contra los objetivos.

Con los drones sucede algo similar pues la estación de control desde la que se guía un dispositivo puede estar ubicada en prácticamente cualquier lugar. El tiempo de respuesta de las fuerzas de seguridad para conseguir identificar al responsable del ataque no permite frenar el ataque e incluso puede a poder identificarlo ante su eventual huida.

Una opción que se puede considerar frente a estas amenazas es intentar limitar el acceso de la población en general a las herramientas con las que llevar a cabo los ataques.

En el caso de internet, se trata de una medida completamente inviable pues, las herramientas necesarias para el desarrollo de las aplicaciones que permiten explotar las innumerables ventajas de las tecnologías de la información son las mismas que pueden ser utilizadas para desarrollar «armas cibernéticas», véase compiladores, herramientas de depuración de software o redes, etc. La imposición de estas limitaciones también

podría suponer un freno al desarrollo tecnológico al reducirse la capacidad de acceder a estas herramientas imprescindibles para crear, analizar, depurar o extender estas nuevas tecnologías.

Con los drones está empezando a ocurrir algo similar debido a la popularización que están experimentando, tanto por la viabilidad tecnológica de su construcción posibilitada con del desarrollo de las tecnologías electrónicas y mecánicas de los últimos años, como por la viabilidad económica de su adquisición asociada a la tremenda reducción de costes que se ha conseguido en estas tecnologías fruto de la propia popularización que ha conducido en muchos casos a economías de escala de los componentes principales.

Las empresas, ante la imposibilidad de dar solución a todos los riesgos a los que se exponen, están recurriendo a cubrirlos mediante contratos de seguro para el caso de que se produzca una incursión en los sistemas, una fuga de datos, etc. que den lugar a pérdidas (de muy diverso origen) en la empresa. Con esta opción se establece un compromiso entre la inversión que la organización está dispuesta a abordar en términos de aseguramiento de sus activos y los riesgos residuales que no serán abordados y que, en caso de producirse, deberán abordarse con la compensación económica del contrato de seguro. Esta alternativa puede resultar viable en un entorno civil y comercial, aunque en un entorno de defensa y seguridad son múltiples los motivos por los que resulta inviable.

Sin embargo, ante un riesgo no siempre es posible contrarrestarlo con la solución tecnológica que lo mitiga de raíz. La utilización civil de las tecnologías duales puede dar lugar a que las técnicas de contramedida lleven asociados unos efectos colaterales que supongan un elevado coste en términos económicos, reputacionales, sociales, etc. que no permitan utilizarlas pese a ser la solución idónea en términos técnicos.

En junio publicaba la Federal Aviation Administration de EE.UU. una advertencia[1] por la que se informaba de que se iban a llevar a cabo experimentos de *jamming* de la señal de GPS en el estado de California. En este mismo documento se especificaba el área

[1] FAA. Flight advisory. GPS Interference Testing CHLK GPS 16-08. https://www.faasafety.gov/files/notices/2016/Jun/CHLK_16-08_GPS_Flight_Advisory.pdf

donde podría producirse la indisponibilidad o la falta de fiabilidad del sistema: un círculo de 253 millas náuticas de radio para alturas a 50 pies sobre el nivel del suelo pero que se extendía hasta las 505 millas de radio a mayor elevación. Para hacerse una idea del tamaño de esta zona puede observarse que, además del estado de California, se veían afectados los estados de Nevada, Arizona y Utah enteros, así como parte de los estados de Oregón, Idaho, Wyoming, Colorado y Nuevo México, además de parte del territorio de los Estados Unidos de México, como se detalla en la figura 1.

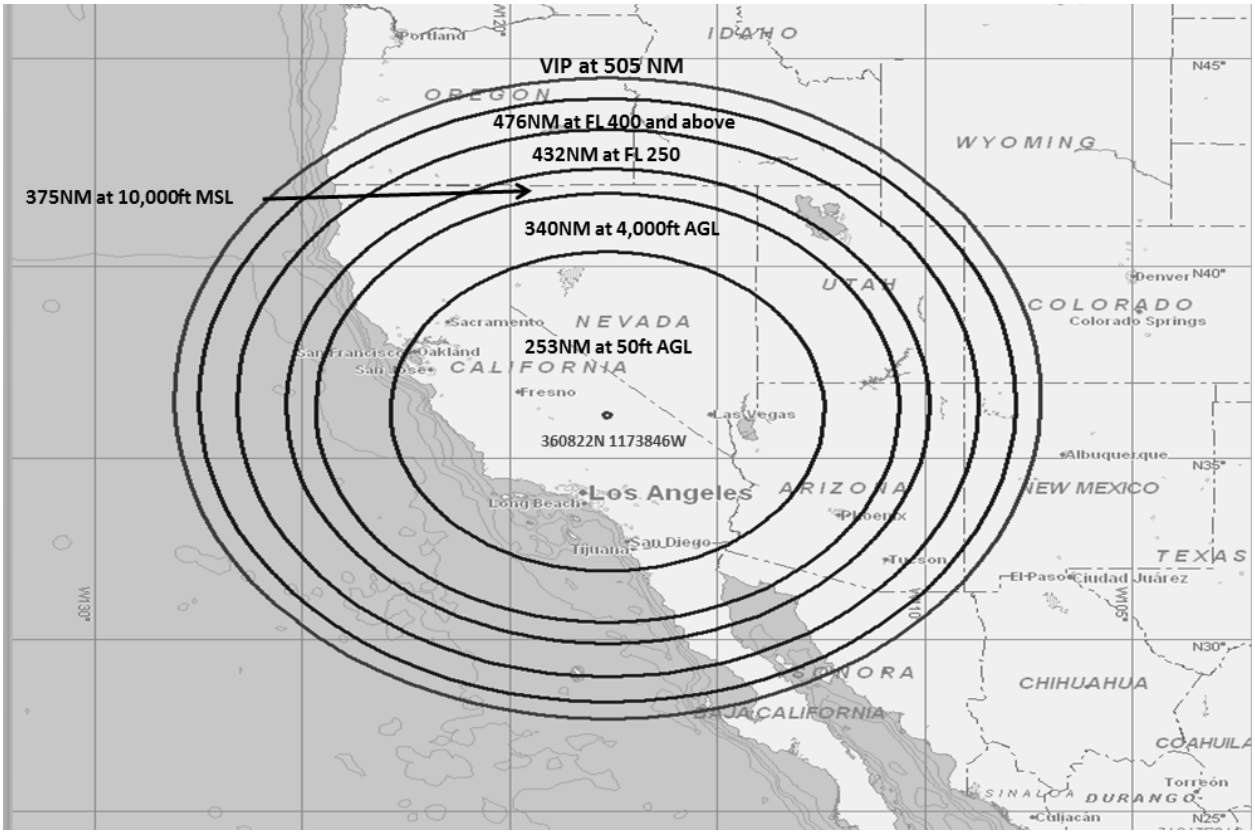

Figura 1 Zona afectada por los experimentos de jamming. (FAA)

Un sistema de este tipo puede ser utilizado por las fuerzas encargadas de la defensa y la seguridad para negar al enemigo la posibilidad de utilizar de forma fiable el sistema, aunque, si esta tecnología cae en manos de terceros, el impacto que su uso puede alcanzar podría afectar a muchos miles o incluso millones de personas y empresas que han pasado a confiar e incluso a depender del correcto funcionamiento del sistema.

Este mismo motivo es el que hace prácticamente inviable la utilización de estas técnicas con fines de defensa y seguridad ante los importantes efectos secundarios que ocasionaría.

En el caso de internet, la utilización de servicios en la nube produce una situación similar en el caso de que se planteara la posibilidad de interrumpir la conexión de un estado a la red con fines de defensa y seguridad. En el territorio de ese estado serían millones las personas y empresas que se verían afectadas, máxime cuando éstas cada vez dependen más de la utilización de sus sistemas informáticos, cuya ubicación es indeterminada, debido a la naturaleza de los servicios de nube que proporcionan los proveedores,y puede estar perfectamente situada más allá de las fronteras de ese estado. Por el mismo motivo, los efectos también podrían extenderse a terceros estados cuyos datos de sus ciudadanos pueden estar ubicados en centros de datos del estado en el que se iba a realizar la desconexión.

Profesionales

Las dificultades que están experimentando los gobiernos a la hora de desarrollar y dotarse de nuevas capacidades, especialmente económicas, ha sido criticado extensamente por la industria como un serio riesgo para el mantenimiento de las empresas de defensa y seguridad. Aquellas con un modelo de negocio más diversificado han sobrevivido mejor ante el difícil escenario que se ha producido, aunque no por ello ha sido posible mantener la plena capacidad en ciertas tecnologías. La falta de contratos de adquisición o desarrollo ha producido el cambio de actividad de personal muy especializado que poco a poco puede haber ido perdiendo los conocimientos y habilidades específicos para el desarrollo de sistemas de defensa y seguridad.

Las características de los nuevos sistemas que se están desarrollando también suponen un reto para los departamentos de recursos humanos a la hora de conseguir los perfiles necesarios para el desarrollo de productos punteros en un entorno muy variable y competitivo tanto en costes como en nuevas prestaciones y capacidades.

La dotación de recursos humanos de las empresas tecnológicas se ha convertido en una búsqueda de talento que va más allá de la comprobación de que se cuenta con un título. A día de hoy es necesario considerar además las habilidades adicionales que presenta el candidato[2]. De esta forma se intenta cubrir un hueco importante que separa la

[2] El Espacio busca talento en las aulas. ¿Contaremos en el futuro con suficientes ingenieros y

formación reglada, imprescindible en muchos casos, de unos conocimientos que difícilmente se incardinan en esta y que solo se adquieren mediante la práctica intensiva del uso de las tecnologías específicas, fruto de haber ocupado un empleo que hacía uso constante de estas capacidades o de haberlas ejercitado con frecuencia por deseo y voluntad del candidato. Este último caso es muy habitual en los profesionales relacionados con la ciberseguridad, donde los conocimientos informales adquiridos motu propio constituyen un activo, en muchos casos insustituible mediante la participación en cursos o actividades formativas regladas. Por esta vía, además de desarrollar hábitos y costumbres de uso que permiten explotar al máximo la potencia de las herramientas disponibles, se genera también una intuición y una capacidad de análisis fruto de un conocimiento amplio y en gran profundidad de los principios en los que se basa el funcionamiento de los sistemas. Estos profesionales son los que cuentan con la capacidad de inducir el cambio gracias a que disponen de un conocimiento más profundo de las capacidades y limitaciones técnicas y tecnológicas.

Sin embargo, también es habitual que estos perfiles presenten carencias en otras facetas como pueden ser la gestión empresarial y la visión estratégica. Aunque no cabe duda de que en estas últimas líneas también es necesaria una elevada capacidad personal para considerar la complejidad del entorno de toma de decisiones, generalmente es más viable conseguir que un técnico adquiera los conocimientos necesarios para que su labor esté alineada con los intereses del organismo en el que desempeña sus funciones, que no intentar que una persona con unos amplios conocimientos de gestión sea capaz de desarrollar las capacidades necesarias para desarrollar, gestionar o analizar la avalancha de tecnologías y evoluciones tecnológicas.

Los recursos humanos constituyen un problema importante para los organismos que ostentan las responsabilidades de defensa y seguridad de los estados. En primer lugar, el personal interno está sujeto a procesos de acceso, selección y promoción cuya flexibilidad es muy limitada. Resulta complicado dotarse de personal con un grado de especialización elevado en un periodo de tiempo reducido, pues debe coincidir la disponibilidad de puestos con el deseo de los trabajadores con los perfiles adecuados de optar a esas plazas. Para hacer frente a este inconveniente puede pensarse en la

científicos? 29/01/2016 https://www.tedae.org/es/noticias/el-espacio-busca-talento-en-las-aulas

contratación de personal externo a la organización para encomendarle la función de gestión e implantación de las medidas de seguridad necesarias. Contar con personal de la empresa privada que posea los conocimientos, experiencia y fiabilidad necesaria para desempeñar su labor en un entorno de defensa y seguridad supone una dificultad importante para las empresas.

Otro inconveniente al que se enfrentan las organizaciones es el de la rotación del personal. En un contexto de personal con elevados grados de especialización, son muchas y diversas las oportunidades que le surgen al personal para abandonar su puesto, de una organización pública o privada, para pasar a desempeñar otro puesto en la empresa privada bajo el incentivo de una mayor remuneración (que puede no ser únicamente económica). Este problema, particularizado para los campos de defensa y seguridad, aunque especialmente para defensa, es aún más grave. Las particularidades del entorno militar requieren contar con personal con una alta especialización además de un conocimiento exhaustivo del entorno en el que desarrollan sus funciones. Por su parte, la dificultad de la gestión del personal público conduce a que estas prestaciones se externalicen en muchos casos. Para disponer del personal con el perfil adecuado, la empresa debe contar con profesionales con mucha experiencia, bien porque la hayan desarrollado individualmente o porque la empresa haya considerado de interés capacitar a sus empleados.

La reducción de la inversión en defensa y seguridad también afectará a los recursos que las empresas estarán dispuestas a invertir para disponer de los perfiles y productos necesarios para satisfacer las necesidades de los organismos de defensa y seguridad. Para paliar esta inversión puede optarse por aprovechar los mismos profesionales que se utilizan en entornos civiles, que tenderán a su vez a aplicar las soluciones que conocen y aplican en el mundo civil en el entorno militar. Mientras que muchas técnicas de ataque y defensa son comunes para entornos civiles y militares, no cabe duda de que la amenaza que pende sobre un organismo de seguridad y defensa puede provenir de entornos mucho más complejos, como otros estados, que pueden contar con presupuestos de ciberseguridad muy elevados.

Puede producirse entre las empresas con capacidad de proporcionar este tipo de servicios una carrera de sueldos para conseguir a los profesionales más experimentados. Esto da lugar a sobrecostes que, en última instancia, deberán ser cubiertos en la factura que las empresas cursan a las administraciones públicas por la prestación de sus servicios. La comunalidad de los conocimientos del entorno de seguridad y defensa respecto a los sistemas civiles que se están implantando da lugar a que los profesionales presenten unas elevadas capacidades, lo que los hace muy deseables para trabajar en el entorno civil, donde la generación de beneficios económicos permite elevar las ofertas a los trabajadores para que se incorporen a generar valor en la compañía. Este camino supone así un hándicap más a la hora de contar en el sector público con una plantilla de personal de elevados conocimientos técnicos a largo plazo.

Conclusiones

Las nuevas amenazas que se deben abordar desde los organismos encargados de la defensa y la seguridad tienen su origen en muchos casos en la democratización que se ha producido en el acceso a la tecnología gracias al enorme potencial industrial y comercial que tienen aparejado. La multiplicación de capacidad que introducen las tecnologías reduce considerablemente el umbral de medios necesarios para poder llevar a cabo un ataque de consecuencias relevantes para la seguridad de la ciudadanía. Frenar estos ataques es un problema creciente porque los medios necesarios son cada vez más complejos y existe una asimetría importante entre los medios necesarios para realizar un ataque puntual frente a los necesarios para conseguir una protección general de los recursos. Además, existen colectivos con una elevada capacidad de inversión que están desarrollando sistemas de ataque muy complejos ante los que es necesaria una elevada y constante inversión para poder hacerles frente.

La línea de trabajo que potencia las tecnologías duales no contribuye a aumentar el hueco entre las capacidades de defensa a las que solo pueden acceder unos pocos, y las capacidades de ataque a las que existe un acceso prácticamente global. De hecho, este hueco se está cerrando poco a poco con la introducción de tecnologías civiles para dar respuesta a las necesidades de seguridad y defensa. La escasa diferenciación tecnológica facilita la labor de explotar los sistemas de defensa y seguridad mediante técnicas desarrolladas para sistemas civiles, que en muchos casos han sido diseñadas

sin tener en cuenta las medidas de seguridad necesarias para su utilización en un entorno hostil.

Se trata de una tendencia que se retroalimenta pues las inversiones en tecnologías específicas de seguridad y defensa cada vez son menores mientras que se hacen cada vez más esfuerzos para aplicar las tecnologías civiles a los problemas de defensa y seguridad. Los conocimientos de los profesionales del sector se concentran en estas últimas y, al igual que a quien tiene un martillo todos los problemas le parecen clavos, ignoran en muchos casos las limitaciones de las tecnologías existentes, anteponiendo la funcionalidad necesaria a las medidas de seguridad imprescindibles para que una tecnología pueda usarse de forma fiable en un entorno hostil.

La Comisión Europea ha identificado la singularidad que supone el desarrollo de tecnologías necesarias para la defensa y la seguridad y ha lanzado dos iniciativas para analizar la inclusión en el próximo programa marco de investigación el desarrollo de tecnologías específicas para la defensa y la seguridad. Primero con el Programa Piloto que ya se ha puesto en marcha y a continuación con la Acción Preparatoria se pretenden adelantar los mecanismos necesarios tanto para poner en marcha líneas de investigación sobre defensa y seguridad como para hacer frente a los múltiples inconvenientes que pueden surgir en un mercado tan singular y tan afectado por los intereses particulares de los Estados que forman la Unión Europea.

David Ramírez Morán
Analista del IEEE